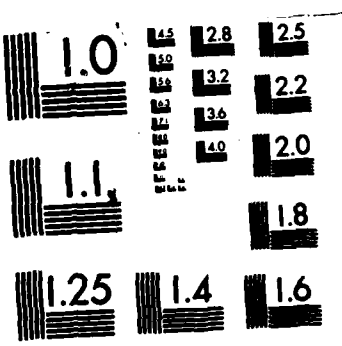
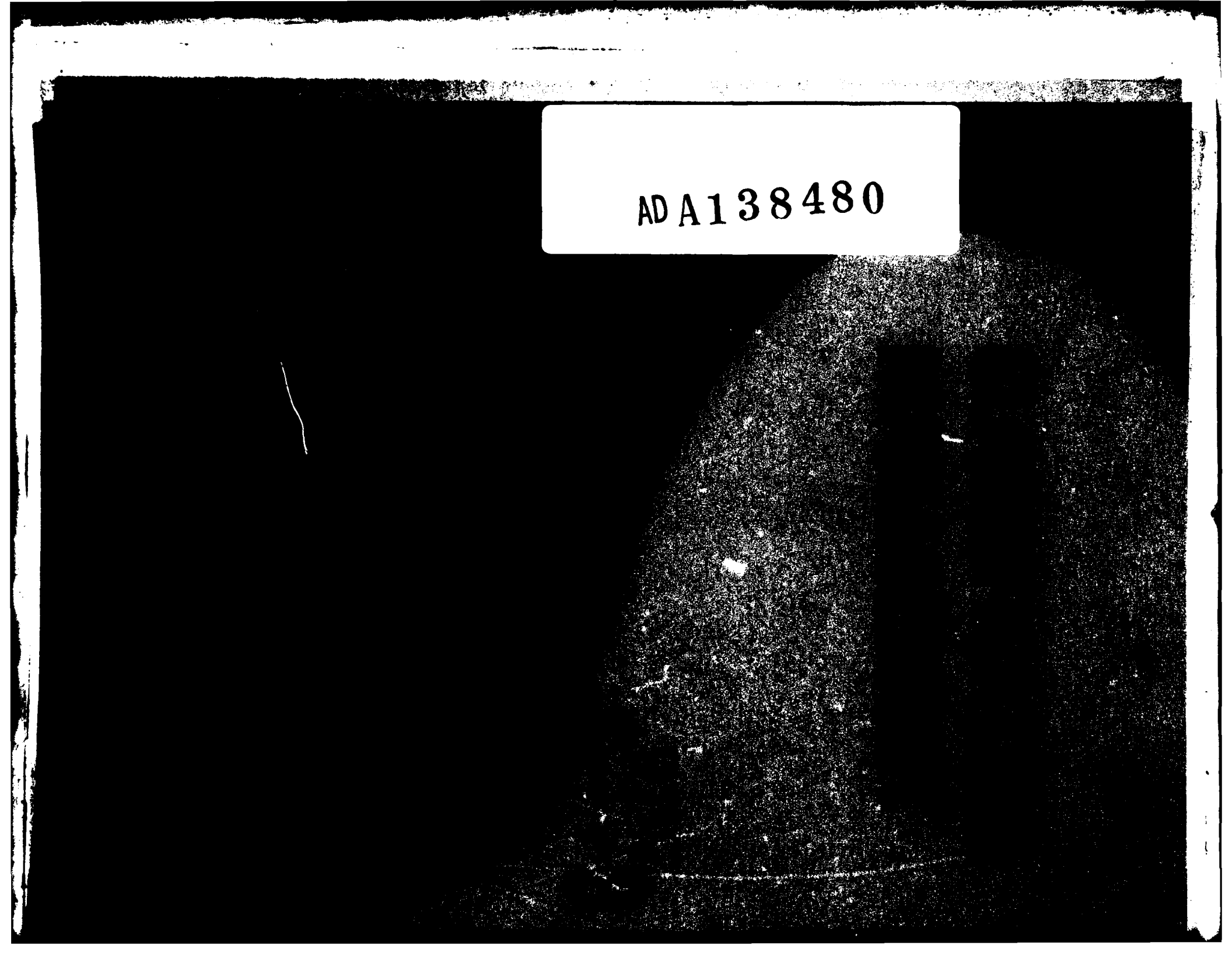
AD-A138 480 CLASSIFICATION MANAGEMENT JOURNAL OF THE NATIONAL CLASSIFICATION MANAGEMENT SOCIETY VOLUME 18 1982(U) NATIONAL CLASSIFICATION MANAGEMENT SOCIETY ALEXANDRIA VA E J SUTO ET AL. 1983 F/G 5/2 NL

1/2

UNCLASSIFIED





CLASSIFICATION MANAGEMENT

Cecil H. Uyehara, Ex. Secretary

JOURNAL OF THE NATIONAL CLASSIFICATION MANAGEMENT SOCIETY
VOLUME XVIII-1982

ISSN-0009-8434

Published by the National Classification Management Society. Mailing Address: Executive Secretary NCMS, 6116 Roseland Drive, Rockville, Maryland 20852. Editors of this volume: Eugene Suto and Muriel Kenney.

TABLE OF CONTENTS:

PART ONE — Proceedings of the Eighteenth Annual Seminar

Operations Security

PART ONE

Proceedings
of the
Eighteenth Annual Seminar

25 - 27 May 1982

Hilton Inn - Florida Center
Orlando, Florida

INFORMATION SECURITY AND TECHNOLOGY TRANSFER (AN OUSD OVERVIEW OF EXECUTIVE ORDER 12356 AND DoD'S VIEW CONCERNING IMPLEMENTATION)

Arthur F. Van Cook
Director of Information Security
Office of the Deputy Under Secretary of Defense (Policy)
Department of Defense

Information Security

Government secrecy in democratic systems has been and remains a controversial issue. It is interesting to step back and look at the U.S. security classification system over the past 30 years to see how different administrations have coped with this issue and the differing methods that have been adopted. Each Executive Order from President Eisenhower's time has been more and more detailed and increasingly complex in its treatment of the principles and rules of security classification. That has changed now that President Reagan has signed Executive Order 12356, "National Security Information," which becomes effective on August 1, 1982. As General Stilwell has just stated, the new Executive Order is more straightforward, and this more direct approach to classification should enhance our ability to protect information that is properly classified.

The Preamble to the Executive Order simply and clearly states the approach to classification: "This Order prescribes a uniform system for classifying, declassifying, and safe-guarding national security information. It recognizes that it is essential that the public be informed concerning the activities of its Government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosures."

Why was the last Executive Order replaced after being in effect for less than 4 years? What does the new Order accomplish? I would like to deal with each of these questions and provide an insight to the workings of the new Order and its impact on the Department of Defense and defense industry.

In dealing with the first question, why another Order? it is well to recount briefly the evolution of this Order. There was foreign concern about the ability of the United States to safeguard secret information that was provided to us in confidence. Foreign intelligence sources were becoming reluctant to share information with us. Also, operating experience with Executive Order 12065 suggested the need for refinements. Thus, in February 1981, the Director of the Information Security Oversight Office (ISOO) called upon the departments and agencies for views on how Executive Order 12065 might be fine-tuned to eliminate any operational problems encountered. Defense and others, except for the Central Intelligence Agency (CIA), responded to the ISOO with fine-tuning proposed changes. Concurrently, CIA formed and AD HOC Intelligence Community Working Group to respond to a White House direction to look at Executive Order 12065 with a view toward enhancing our intelligence collection capability. The group began fixing Executive Order 12065 and wound up rewriting the Order from the preamble on to the end. The proposed replacement Order was sent not only to the ISOO as the CIA response but also to the White House for approval for formal coordination. The CIA Working Group's proposed replacement Order became the foundation paper for the formal coordination effort undertaken by the ISOO.

What does the new Executive Order accomplish? I have already provided some insight into what Executive Order 12356 does. It prescribes a uniform system for classifying, declassifying, and safeguarding of national security information. It is practical, easy to work with because it simplifies the classification rules and markings; permits, when necessary, the long-term protection of information in the interest of national security; continues a strong oversight mechanism; and retains the best features of the past Executive Order such as the two-step process for determining whether information should be classified.

Beyond these points, the new Executive Order enhances protection for national security information without permitting excessive classification of information by the Government. It continues to recognize that Americans need to be informed about their Government's activities, and it also recognizes that it is essential to protect certain sensitive information when uncontrolled disclo-

sure could harm the security of all Americans. Executive Order 12356 establishes improved standards and procedures to achieve the proper balance between these two important objectives and permits the Government to classify only that information where unauthorized disclosure could reasonably be expected to damage America's security.

To assure that the proper balance is maintained, the fundamental prohibitions against the use of classification are carried over to the new Executive Order. For example, basic scientific research not related clearly to the national security may not be classified. Further, given the Order's definitions, basic scientific research that is related clearly to the national security may not be classified unless the Government owns that information. Also, the Order expressly and properly prohibits use of classification to hide violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the public release of information that does not require national security protection.

In talking about changes reflected in the new Executive Order, when comparing its provisions with those of Executive Order 12065, one has to mention the changes in tone first. Where Executive Order 12065 was somewhat negative in its approach, Executive Order 12356 is quite positive. This shift is syntax is important because, as President Reagan said when he signed the Order, "Protection of the security of the United States and all its citizens is the first and most solemn duty of every President. This Order will improve my ability to meet this Constitutional obligation..." In other words, I think that we had progressed from one order to another to the point where there was little or no mesh of the security classification system with practical real-world needs. The new Executive Order makes no apology about the need to classify some information is the interest of national security. It is my expectation that we have in Executive Order 12356 an enduring classification system in its fundamentals— one that will allow us to keep our adversary in the dark without keeping Americans from the light.

The salient features of Executive Order 12356 are many — some new some and old. The Order continues the three-level classification system though not without some change. The "Confidential" classification now means that the unauthorized disclosure of the information so labeled reasonably could be expected to cause "damage" to the national security whereas the standard was "identifiable damage." Critics of the Order have suggested that this change will cause the classification of more information, but I have to disagree. The two-step process leading to a classification decision is still in place. That process requires that a determination be made that the information being considered for classification is indeed within one of the several catagories of information that is classifiable. Having passed that test, it is next necessary to conclude that damage to the national security will occur in the event of unauthorized disclosure of the information. In reaching this conclusion, one must naturally envision what that expected damage will be. If you foresee the damage, the decision will be to classify the information. But note that in this thought process, you have mentally identified the damage. Thus, I believe that change from "identifiable damage" to just plain "damage" will have no impact on the amount of information being classified. What then does this change accomplish? Simply put, it removes a contentious adjective that probably was never needed in the first place.

Imagine that you do not have original classification authority. Imagine also that you have a doubt about whether to classify or doubt about the level of classification that should be assigned to information you are developing. The new Executive Order prescribes that in these circumstances the information shall be safeguarded as if it were classified or safeguarded at the higher level of classification. Safeguarding as used here is distinct from classification; an original classification authority shall make the classification determination within 30 days in accordance with the Order. This changes the past approach which was, when in doubt, use the less restrictive treatment.

Under Executive Order 12356 original Top Secret classification authority may be granted by not only the President of the United States and Secretary of Defense, and other similar officials, but now also by the senior agency official desig-

nated by the agency head pursuant to the Executive Order requirement. That senior agency official for the Department of Defense, not including the Military Departments, is the Deputy Under Secretary of Defense (Policy), General Stilwell. This change will result in a reduction of the administrative burden on the Secretary of Defense; there will be less paper work, but the same degree of control being exercised over who may be authorized to originally classify information in the interest of national security.

The Order's listing of classifiable categories of information has been expanded while none was dropped as compared to the last Order. The new categories are:

- "the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security";
- "special activities" has been added parenthetically to the existing categories concerning intelligence activities, or intelligence sources or methods;
- "cryptology"; and
- "a confidential source."

The added category concerning vulnerabilities may appear to overlap that pertaining to military plans, weapons, or operations. Appearances notwithstanding, this added category, like the others, is intended to provide a sounder basis for classification of, for example, information regarding the physical protection of the President. We can rely on the recently issued Executive Order 12333, which governs intelligence activities, for a definition of "special activities"; and the classification Order defines a "confidential source" as meaning "any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence." Here again I do not envision a marked increase in the amount of information that will be classified.

Even though the two-step classification process has been retained, it has been modified in two areas — tone and substance. The tonal change takes this provision from a negative to a positive statement; that is, if information is determined to concern one or more of the classifiable categories it shall be classified when a damage determination is made. The substantive change takes into account the reality of the existence of other information. That is, when considering the question of whether to classify, the Order provides for a determination by the original classifier that unauthorized disclosure of the information, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security. What we have here is Executive Order-level recognition of the so-called compilation theory, long practiced in the Department of Defense in special circumstances.

The "presumption of damage" provision has been expanded to include intelligence sources or methods, along with foreign government information, and the identify of a confidential source. Doing so takes cognizance of the sensitivity and perishability of intelligence sources and methods. The practical impact of the "presumption of damage" section of the Order is the setting aside of the second step of the two-step classification process.

The new Executive Order specifically provides that classified information shall be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or aboard of identical or similar information. The last Order had no similar provision.

Perhaps the most significant change brought about by the signing of Executive Order 12356 involves the duration of classification. Now, information shall be classified as long as required by national security considerations. When it can be predetermined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified. Closely related to this change is the fact that any original classification authority — whether at the Confidential, Secret, or Top Secret level — may set any date or event for declassification. Gone are the artificial 6-and 20-year limitations that substituted for judgment of original classification authorities.

The Order provides that the otherwise required markings may be omitted when the markings themselves would reveal a confidential source

or relationship not otherwise evident in the document or information. At the time of original classification, the following markings are required:

- one of the three classification levels;
- the identity of the original classification authority if other than the person whose name appears as the approving or signing official;
- the agency and office of origin; and
- the date or event for declassification, or the notation "Originating Agency's Determination Required."

The specific requirement to identify the agency of origin is new, but this should have no impact in most cases. The other new requirement here is the notation "Originating Agency's Determination Required" which is abbreviated as "OADR."

Required portion or paragraph classification marking survived an early struggle during development of the new Executive Order. That struggle, however, lead to a compromise; that is, the requirement may now be waived for specified classes of documents or information by agency heads rather than the ISOO Director. This is another area where only time will tell the true impact of this change. My concern is that there may be wholesale waivers granted by non-DoD agencies that will have an adverse impact on DoD derivative classification actions. I expect that there will be few, if any, waivers of the portion marking requirement within the Department of Defense.

Derivative classification is carried forward just about as it was stated in the last Order. But the provisions regarding security classification guides have changed — more than 1,200 guides are the source of a great deal of derivative classification in the Department of Defense. Under Executive Order 12356, classification guides shall be approved personally and in writing by an official who (1) has program or supervisory responsibility over the information or is the senior agency official designated as such pursuant to the Order; and (2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

No longer must all guides be approved by a Top Secret classification authority, and the requirement to issue them may be waived by agency heads for good cause. Such waivers are to be reported to the ISOO Director. Here again, I anticipated few if any DoD waivers.

Systematic declassification review programs on the part of the agencies and departments were required by Executive Order 12065. Under that Order most permanently valuable records were to have been reviewed as they became 20 years old, while foreign government information was to be reviewed at age 30. Under the new Executive Order all that has changed. Systematic declassification review is now required only at the General Service Administration's National Archives and Records Service (NARS). It is an option elsewhere. The Order specifies that the required systematic review shall be in accordance with procedures and timeframes prescribed in the directive of the ISOO implementing the Order, which now states that permanently valuable records will be systematically reviewed for declassification at age 30, except that intelligence material will be reviewed at age 50. The NARS review will, as before, be conducted on the basis of agency developed declassification guidelines.

What is the Department of Defense going to do now that systematic review is optional? It is our intention to support continuation of those well-established systematic review programs for they have made a considerable amount of historically significant information publicly available. Moreover, given the optional nature of systematic review by the agencies, we will be able to focus our efforts on those subject areas known to be of general public interest and those areas where we can attain a high payoff in terms of declassified information.

The safeguarding portion of the new Executive Order has been simplified considerably. Gone is the long treatment of the detailed requirements pertaining to reproduction controls. The Order's requirements regarding the creation of special access programs have been abbreviated; nonetheless, the provisions essential to adequate control of special access programs remain. As before, the implementing directives of the ISOO will contain many of the safeguarding nuts-and-bolts provisions.

Now, it can be seen that the new Executive Order will have no adverse impact in the Department or defense industry. As before, the ISOO will be promulgating a Government-wide implementating directive. It is not yet final, unless Judge Clark, the Assistant to the President for National Security Affairs, has given his approval and Mr. Garfinkel, Director of the ISOO, has signed the directive since I left Washington.

While the new Executive Order was in its final processing stages, the ISOO was putting the finishing touches on its draft implementer that was provided to the departments and agencies along with the signed Order on April 2. As was the case with the Order, my office coordinated the draft ISOO directive throughout the Department. The results of that process were 45 comments spread over 12 pages, intented to make implementation of the directive, and thus the Order, more efficient and effective in the Department as well as in industry. Our comments and rationale for changing the draft directive were explained personally to Mr. Garfinkel and his staff before being finalized for General Stilwell's signature on behalf of the Secretary of Defense. This extra step was worth the effort, as virtually all of our recommended changes have been accommodated. The understanding and constructive cooperation displayed by Mr.Garfinkel and his staff during this coordination process was outstanding, and the Department is most appreciative of that show of cooperation.

Two areas of the ISOO directive of particular interest to industry and most Government personnel deserve mention. First, the directive and the Order cause no basic change to the derivative classification and marking systems. The familar "Classified by" and "Declassify on" lines remain in place though the "Declassify on" line will now be completed with "OADR" when appropriate. The "Review on" line disappears from the scene. Second, the safeguarding nuts-and-bolts of the directive are substantially as they have been. As in the case of the new Executive Order, I believe the ISOO directive will have a favorable impact on the Department and defense industry.

That leaves the Department's Information Security Program Regulation and the Industrial Security Manual (ISM) and Industrial Security Regulation (ISR). Will they be changed extensively?

While the new Executive Order and ISOO directive were being developed, we were concurrently looking at the Information Security Program Regulation to access where and to what extent it would require change. Those who are familiar with the Regulation will recognize the need for many changes. But, most of those changes, taken one-by-one, are not dramatic in light of what has already been covered. Though most of the Regulation changes are driven by the Order and draft directive, the opportunity to make other refinements based on operating experience has not been lost.

The internal DoD coordination of the Regulation changes is essentially complete, due in large part to the opportunity to discuss personally the Department's position on the draft directive with the ISOO Director. That discussion enabled us to proceed with the Regulation coordination effort at an early date with fairly certain knowledge that we were going down the right road. I must also add, that I made the proposed Information Security Program Regulation changes available to the President of your Society for review, and I asked that he arrange for a meeting with Society industry members in my office so that I could hear personally their views on the Regulation changes. This was done. The prospect of no retroactive re-marking requirements was greeted with enthusiasm. Beyond that, just let me say that the new Regulation will be a better product as a result of that meeting.

As for the ISM and ISR , there will be relatively few changes simply because most of the differences between Executive Orders 12065 and 12356 occur in the area of original classification — a Government responsibility. I can tell you now, given prompt approval of the ISOO directive, that the Information Security Program Regulation will be on the street well before the Order's August 1 effective date. It is my sincere desire to have the ISM, ISR, and DoD Component Supplements ready by then as well.

Technology Transfer

The Department of Defense has been concerned for some time about another security related sub-

ject — technology transfer and the loss of military operational data. There is a virtual unremitting flow of unclassified defense information to our adversaries. This hemorrhage of information to hostile nations, particularly technology and technical data with military application, is one of the more serious problems confronting the Department.

Soviet bloc acquisition of unclassified national security related publications greatly enhances their capabilities to design, produce, and field weapon systems of all types, as well as develop measures to counter U.S. weapon systems. It cuts their production costs, shortens their production times, and improves the quality of their products.

A Soviet scientist who defected several years ago told Congress that the majority of Soviet information collection requirements can be openly obtained in the United States. The Federal Bureau of Investigation has estimated that as high as 90 percent of the Soviet collection requirements can be satisfied through open sources. A recent unclassified Central Intelligence Agency (CIA) report states that Soviet intelligence organization have been so successful at acquiring western technology that the manpower levels allocated to this effort have increased significantly since the 1970s to the point where there are now several thousand Soviet bloc technology collection officers at work.

We are painfully aware of Communist bloc efforts within the United States to obtain technology, mostly through legal means, that is, through open literature, which we are powerless to stop. Prior to February 1980, for example, we stood helplessly by as the Soviet Union purchased 80,000 technical documents from the National Technical Information Service (NTIS). Although their access to the NTIS has now been officially terminated, Soviet surrogates undoubtedly continue to exploit this source of extremely valuable information.

Members of Congress, industry spokesmen, and the media frequently lament this state of affairs, and ask, "Is there nothing that can be done?" Generally, these activities are carried out overtly and do not violate existing U.S. law. In fact, it has always been presumed that little could or should be done to limit such acquisitions, relying instead upon the ability of the publishers of such documents to properly secure sensitive information by using the security classification system. However, much of this information is not classifiable under the rules of either Executive Order 12065 or 12356. The existing classification system does not provide protection to a large body of sensitive national security information, particularly militarily critical technology and operational data developed solely for the use of our armed forces.

Classification of such information has been neither possible nor practical. Although such sensitive national security related information fits within the categories permitted to be classified, the impact of its uncontrolled dissemination does not rise to the level of the "damage" standard of the Executive Order. Disclosure of the technical characteristics of electronics components used in a missile guidance system, for example, may not appear to damage the national security, and yet may provide our adversaries with precisely what they need to produce a more effective missile. It is this "damage" standard that is applied by originators in deciding whether to make their documents unclassified or to protect them by security classification. Uppermost in their mind is the realization that the test for classification could receive judicial review. Consequently, if a determination is made not to classify, this information is vulnerable under the Freedom of Information Act (FOIA), since the information does not fall within one of the non-security exemptions to mandatory disclosure. It therefore becomes available and this valuable technological and operational information can be utilitized by our adversaries to their military benefit.

The trend toward openness in government has run virtually uninterrupted for the past 30 years. It is a trend that the Department of Defense certainly has supported over those years. It has long been the Department of Defense's policy not to constrain information that the public requires to be informed sufficiently about the activities and operating functions of the Department. We were concerned, however, that there appeared to be no compelling reason for permitting government pub-

lications that are required solely for official use, or for strictly administrative or operational purposes, to be freely transferable to all countries participating in the recently rediscovered International Exchange Program, even though the publications were not classified for reasons of national security.

What has been and what is being done about all this? The Military Departments and Defense Agencies were asked to revise their policies and procedures with respect to the approval and issuance of unclassified field manuals, technical manuals, and other publications containing valuable technical data to assure that these publications, required solely for official use or for strictly administrative or operational purposes, were clearly identified. Further, the Library of Congress and the Government Printing Office agreed not to include Defense documents so identified in the International Exchange Program. Our aim was not to exclude all Defense documents from the Program but to provide more positive control over a certain class of such documents. This we did.

Not satisfied that we had done all we could within the department to limit the availability of such unclassified information, the Deputy Secretary of Defense (Policy) established a DoD Working Group on Technology Transfer. This Group which I was asked to chair, was directed to address (1) what the Department of Defense can do now to effect more positive control of such Defense information, (2) what Department policies and procedures should be changed to effect more positive control, and (3) what we can ask others outside the Department to do to assist in these efforts?

The issues involved in such as undertaking are not unfamiliar and center around the contervailing principles of openness in government and the Government's legitimate need to protect from disclosure certain information in the interest of national security. What we are seeking is a more equitable balance between the need to protect certain information and the competing need to keep the public properly informed about the activities of its government.

One of the initiatives that emerged, as a result of efforts of the DoD Working Group on Technology Transfer, was a proposal to authorize the Secretary of Defense, by Executive Order, to classify at a level lower than Confidential, Defense information where unauthorized disclosure could reasonably be expected to be prejudicial to the national security because it could result in the loss to the United States of a military technological or operational advantage. This, and our earlier proposal to establish a fourth level of classification —"Restricted," did not receive broad Executive Branch support and have been abandoned.

Another initiative appears in the Defense legislative proposal, to amend the FOIA, where it has been recommended to exempt from mandatory disclosure technical data that may not be exported lawfully outside the United States without an approval, authorization, or a license under Federal export laws. This recommendation is now a part of the Administration's proposal to amend the Act and, from last week's press accounts, it has cleared the Senate Judiciary Committee intact.

Further internal proposals to provide more positive control of this type of information that are allowable under existing policies and procedures are being developed, but it would be premature to discuss them at this time since they have not been fully coordinated within the Department.

GAO'S CONTINUING REVIEW OF THE INFORMATION SECURITY PROGRAM

Irving T. Boker
U.S. General Accounting Office

It's a pleasure for me to be a part of this seminar, representing the General Accounting Office (GAO).

GAO's continuing reviews of the Government's Information Security Program have led us from oversight of the Program by the Interagency Classification Review Committee and the Information Security Oversight Office, to systematic review for declassification, to classification management in industry and at military installations, to delays in the processing of personnel security clearances, and finally, to Special Access Programs and Carve-Out Contracts in industry. In fact, the secrecy of these special programs and contracts has restricted our review efforts.

I realize that many of you know first-hand about Special Access Programs and Carve-Out Contracts. However, there are probably many who are unfamiliar with these terms. So, for this latter group, let me take a few minutes to explain the terminology and provide some background information that should make it easier for you to understand my discussion this morning and perhaps be useful to you in the future. I don't pretend to be an expert in this field. Consequently, I welcome and corrections or clarification of my remarks.

Special Access Programs

First, let's look at Special Access Programs. Executive Order 12065, which took effect December 1, 1978, to my knowledge, is the first Order to recognize Special Access Programs. It provides criteria for their establishment; procedures for their initial approval by agency heads; and revalidation, as to their continued need, at 5-year intervals. The agency heads authorized to approve Special Access Programs in the Department of Defense (DoD), in addition to the Secretary of Defense, include the Secretaries of the Air Force, Army and Navy. Special Access Programs pertaining to intelligence activities are to be approved by the Director of Central Intelligence. What is a Special Access Program? The Executive Order says that it is a program that may be created or continued only on a specific showing that (1) normal management and safeguarding procedures are not sufficient to limit need-to-know or access, (2) the number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information involved, and (3) the special access controls balance the need to protect the information against the full spectrum of needs to use the information. Each agency is required to establish and maintain a system of accounting for such programs. The DoD Information Security Program Regulation, 5200.1-R, amplifies the above requirements, as do the regulations of the military services and other DoD components. Information on all Special Access Programs is required to be submitted to the Deputy Under Secretary of Defense for Policy. The new Executive Order 12356, which takes effect August 1, makes some major changes. The criteria for establishing the programs has been eliminated, as has the need for revalidation every 5 years. The new ISOO Directive for implementing the Order does require agencies to consider the adequacy of normal safeguarding procedures and the number of persons who will require access, before authorizing or continuing a special program. Agency heads are still required to approve new programs in writing and to maintain a system of accounting for all Special Access Programs. As in the previous Executive Order, programs related to intelligence activities require the approval of the Director of Central Intelligence.

There are two basic types of special programs: those that contain intelligence or intelligence-related information and those that don't. Intelligence or intelligence-related information that requires special handling is referred to as Sensitive Compartmented Information or SCI. Special facilities known as Sensitive Compartmented Information Facilities (SCIFs) are required for the storage of SCI. I will discuss the SCIFs in more detail a little later on. There are a number of Special Access Programs that do not involve intelligence-related information. However, some of the program information, because of its sensitivity, is kept in SCIFs, or as they are sometimes called, vaults or tanks. There is standard guidance on SCIF construction and the protection of SCI for that group of Special Access Programs. There are no such standards for protecting nonintelligence related Special Access Program information. Although some DoD groups have issued guidance for their own programs.

Carve-Out Contracts

Another term, often confused and thought to be synonymous with Special Access Programs, is Carve-Outs or Carve-Out Contracts. To the best of our knowledge this term has not been defined in the DoD Industrial Security Regulation or Industrial Security Manual. Implementing Regulations of the Military Services do use the term Carve-Out and have done so for many years. For example the 1972 Edition of the Air Force Regulation on participation in the industrial security program defined Carve-Out. It said, "On rare occasions there may be a project of such high degree of sensitivity that additional controls must be provided to insure the

required a degree of security. When the project also involves the award of classified contract, that contract may be excluded (sometimes referred to as a Carve-Out) from the usual pattern of supervision by the cognizant security office." The cognizant security office in 1972 was the Defense Logistics Agency. Since October 1980, the Defense Investigative Service (DIS) has been responsible for administering the Defense Industrial Security Program.

In mentioning the Air Force Regulation, I was not trying to single out the Air Force. In fact, that same Regulation, in the section preceding the one that I just quoted, had some very sound theory. I would like to read that section to you now:

"The DoD Industrial Security Program is designed to provide for the security of classified Defense information in the possession of industry. This Program offers increased security effectiveness by providing uniform policies, practices, and procedures for industry, which are established by a single agency. Anything which tends to fragment or divide the Program and requires different security guidance for its various classified contracts results ultimately in a weaking of security. For this reason, all Air Force classified contracts normally fall within the purview of the DoD Industrial Security Program."

So those who didn't know what a Carve-Out Contract is, now know that it is a contract for which security administration is maintained by the DoD organization that awarded the contract. That also means that, in addition to the requirements of the Department's Information Security Regulation, Industrial Security Regulation, and Industrial Security Manual, the organization awarding the contract may lay additional security requirements on the contractor, such as storage requirements and limited personnel access. As you can see, these Carve-Out Contracts adhere to the requirements of Special Access Programs. Now, let me add a couple of wrinkles to this seemingly logical flow of programs and supporting contracts. Wrinkle Number 1: Not all Carve-Out Contracts are in support of Special Access Programs. How many contract are there like that? Nobody knows. Contractors, generally, have no way of knowing whether they have a legitimate Carve-Out Contract. Wrinkle Number 2: Some contracts supporting Special Access Programs are not Carve-Out. The DIS still maintains security cognizance. DIS inspector are "read on" to the contracts, kust like the contractors' employees. Presumably, in most cases, each individual, either contractor or Government employee, is required to sign a statement that he or she has received a security briefing and fully understands the penalties for disclosing any program or contract information to any individual not authorized to receive it. Access lists or rosters of all individuals who have been cleared for the program or contract, on a need-to-know or must-know basis, are also maintained by a special security officer. After the individual has completed his or her work in the program, another statement has to be signed which acknowledges that the individual has been debriefed, does not have possession of any program information, and will not disclosed any information to any unauthorized individual or agency. Now that I've confused those of you who were not familiar with Special Access Programs and Carve-Outs Contracts, I want to talk a little bit about what GAO has done in this area.

GAO's General Approach

Our work is usually done in two phases — a survey and a detailed review. GAO is considerate of its auditors; it offers training programs aimed at improving our auditing and writing skills. Our training program for National Security information is on-the-job training and attendance at these seminars. So our survey in any area of national security information is, to a good extent, training and education. In addition to obtaining general information about the area, we look for things or conditions that appear to need improvement. After identifying these conditions, we plan the type and extent of work that we think will be necessary to convincingly support any conclusions or recommendations. After completing the survey, we proceed to the second phase or work, the detailed

review. Sometimes, after completing the survey phase, we decide that a detailed review is not warranted. There may be several reasons for the decision. For example, we may be unable to identify any potentially serious deficiencies. Or, the Agency may have already initiated some corrective measures for the deficiencies that we identified.

Last December we started a survey entitled, "Evaluation of Industry Security for DoD's Carve-Out Contracts and Special Access Programs." The audit team, Jim Moses from our Los Angeles office and Jim Reid and I from our Headquarters Office, thought that three months would be sufficient time to complete a survey. We thought wrong —for several reasons. For one thing, the special program area is much larger than we anticipated. Another problem — about half of the programs and contracts are not centrally controlled. Finally, we had a problem in an area where we anticipated some difficulty — access to records. These problems, plus the diversity of administrative handling of Special Access Contracts, and the time needed for us to get educated have delayed the survey several months. With respect to education, I would like to publicly thank DoD and industry security officials for their patience and help during this very trying period for us. We unanimously agree that this is the most difficult and frustrating assignment that we have ever done in our GAO careers. I guess if you want to look at that another way, it's a plus for the overall security of these Special Access Programs in industry.

Our survey has three broad objectives: (1) Was there adequate assurance that special program information entrusted to industry was properly protected; (2) was there some potential for providing adequate security more efficiently and economically in DoD and industry; and (3) were there many Carve-Out Contracts that did not support Special Access Programs and did not warrant the added security requirements? We established certain limitations and groundrules for our work. We were not concerned with program data, only with security requirements. Generally, we limited our survey to the Army, Navy, and Air Force, but we planned to identify any inconsistencies with other Defense Components and Government Agencies. We planned to visit about 30 contractors on the east and west coasts. The military services would not be advised of any information, complaints, or suggestions made by special contractors. Obviously, DoD officials knew where we were going when our clearances were passed, but they had no way of knowing which contractor said what, at least not from us. We agreed to discuss any overall deficiencies noted with the appropriate service.

Survey Results

Sensitive Compartmented Information (SCI) Contracts — We started with contracts involving SCI maintained in SCIFs, tanks, vaults, or whatever you want to call them. The military services were very cooperative. Generally, we had no difficulty in identifying the contractors with SCIFs and the number of contracts with each. We also had no problems reviewing the special access listings, the DD Form 254s, and some inspection reports. We visited contractors and DoD special security officers (SSOs). If you reshuffle those letters, you get SOS. We think, and industry representatives generally agreed, that the SSOs, although limited in number, do an outstanding job answering SOS calls from their counterparts in industry, the CSSOs, or Contractor Speical Security Officers. The CSSOs and their alternates are responsible for controlling access to the SCIFs and the safes within the SCIFs were sensitive information is stored. Some SCIFs have many separate areas for individuals with special clearances to work with the information.

Sensitive Compartmented Information Facilities (SCIFs) — the Defense Intelligence Agency has issued standards for SCIF construction and administrative security. The agency also inspects new SCIFs to certify that the standards are met. The construction standards are minimum standards. Consequently, the Military Services do, on occasion, require that SCIFs be constructed to higher standards than the prescribed minimums. Some contractors commented about the different standards among the services. Others commented that design and construction of the SCIFs was not preceded by a threat analysis. Certainly the objective of maximum security is commendable. But how much is enough and how much is too much? And the costs of these excesses can, add up in the aggregate. SCIF construction costs can range from $10,000 to $1 million. One contractor secur-

ity manager told us that the company was constructing a SCIF for one of the services, at an estimated cost of $100,000. However, because the company was hopeful of receiving a contract or contracts from another Defense Component, the SCIF was being constructed to that component's requirements, thereby increasing the cost by an additional $25,000.

Let me give you an example of a visit to a typical SCIF. First, you arrive at the contractor's building, where you are required to show identification upon entering. Then you wait for an individual to escort you in the building. When you finally reach the SCIF, which is usually hidden away in some out of the way place, you find a door with a combination or cipher lock. Of course, the door is equipped with an alarm system, and any attempt to enter the room while the alarm is on will bring a security guard. Once inside that door, you see something resembling a bank vault, a reinforced door with a combination lock, and another alarm system. Inside the vault, there are sensors to detect movement. Sometimes there are sensors outside the vault, as well. The CSSO and an alternate CSSO often are the only contractor employees who have access to the safes.

While on the subject of safes, the Intelligence Agencies require separate safes, while the Military Services require separate drawers for their contracts. Sometimes, even a separate drawer for each contract, and sometimes each drawer has its own combination lock. If only two contractor employees — the CSSO and the alternate CSSO — have access to the safes, are all these extra precautions needed? How much is enough? This type of situation was especially repugnant in one case. The Security Officer told us that collectively, several contracts had a total of about 150 SCI documents. Yet there were five, five-drawer safes in the vault. But safes are really one of the nominal costs involved in a SCIF. Construction requirements are the biggest element of cost, followed by intrusion systems. If the SCIF must contain a computer or word processors, the cost of the added construction requirements skyrockets because of additional security standards.

Memorandums of Agreements and Inspections

I don't want to be totally negative. There have been successful efforts among the Services and the Intelligence Agencies to use space in each other's SCIFs. Every SCIF has a Sponsoring Agency or Group. For example, the Navy may be the sponsor of a new SCIF. The SCIF is constructed to Navy requirements which must meet the minimum DoD standards. As a SCIF sponsor, the Navy assumes responsibility for the annual physical and technical inspections that are required. If another DoD Component or one of the Intelligence Agencies also awards a contract to the company and the contract involves SCI, arrangements can be made to use the Navy -sponsored SCIF. The two groups enter into a Memorandum of Agreement, popularly called an MOA. The second group, the tenant group, is usually called an MOA. An inspection team from the SCIF sponsor, in this case the Navy, makes an annual physical and technical inspection and checks on Navy documents in the SCIF. The other DoD components and other Agencies are responsible for inspecting their own classified documents. We understand that coordination of physical inspections is a relatively recent development — and improvement. Many of the SCIFs have more than one MOA or tenant. Many contractors have more than one SCIF. Several have as many as four or five SCIFs at the same plant location or in some cases, even in the same building.

Observations

Since we have not formally conveyed our findings to the top DoD officials, it would be inappropriate for me to air them in detail at this forum. I can say that we did observe some deficiencies in control procedures that we discussed with officials of the Military Services, and they concurred. Inconsistency seems to be the name of the game at all levels — from overall program administration to particular contract requirements. I don't want to fan the flames of the double standard often voiced by Industry Security Officials, but we couldn't help noticing a major difference in the required frequency for SCIF inspections. SCIFs at Military Installations require an inspection at least once every 3 years, or sooner, if the need arises. On the other hand, industry SCIFs must be inspected every year. We're not advocating a 3-year rule for industry. we're just noting the inconsistencies. A further inconsistency is the National Security Agency inspection cycle. NSA inspects industry SCIFs 3 or 4 times a year, not withstanding the fact

that some of the information that it maintains in the SCIF may be similar to the level or type of information that a Military Service maintains in a SCIF, or even in the same SCIF. NSA officials told us that their visits cover more than just inspections. Their visits, among other things, include training and orientation for contractor employees and assistance in resolving problems.

Nonintelligence Related Special Access Contracts

Earlier I mentioned that other category of Special Access Programs, those not related to intelligence activities. We had an interesting experience in this area. We had always thought that, generally, intelligence related activities were the most sensitive part of our national security information. That's why the data is maintained in SCIFs. Of course there are exceptions. There are some very sentitive R&D programs. As I also mentioned earlier, the Military Services were cooperative in providing contract data on the SCI programs. So it was somewhat of a shock to us when we tried to get contract data for the nonintelligence programs, and we encountered considerable resistance. You wouldn't believe, nor do I want to take the time to recount all the problems. One service did give us some data on contractors and special programs, but we were not permitted to review the files ourselves. Therefore, we had no assurance that the data given was unsanitized or complete. We later discovered that some of the data was incomplete. A second service at first denied having any Nonintelligence Special Access Program Contracts. After many telephone calls, they finally acknowledged two nonintelligence related programs with Carve-Out Contracts. The third service denied us access to any contract data and suggested that its own auditors do the job for us.

While on the subject of Nonintelligence Related Special Access Programs, I'll tell you a little story about one of our visits to a contractor's plant. About a year ago when we were doing our review on delays in getting personnel security clearances processed, we were talking to a security manager in his office, which was just off the main work area. We were not in a SCIF. I don't recall any special protective devices for, or in, the office except for a five-drawer safe. One thing did catch our eye, though. Two drawers of the safe had plastic labels with large letters that said "Carve-Out Material Only." Of course, after we started our suvey of Special Access Contracts, we revisited the contractor. The Security Manager told us that the labels has been put on by his predecessor and didn't mean anything, because the company did not have any Carve-Out Contracts. We did not insist that he open the safe to prove it, because we didn't want to imply that we didn't believe him. In retrospect, I'm sorry that we didn't force the issue. However, since the Security Manager said that they had no Carve-Out Contracts, I asked for the two labels as a souvenir, and he gave then to me. Here's one of them. This is an interesting story for two reasons. First, it shows poor judgement on the part of the Security Manager, identifying where Carve-Out information might be. Second, during security inspections, the Government Inspector should have suggested that the labels be removed.

Conclusion

Industry, and subsequently the Government, is spending hundreds of millions of dollars annually on physical security, usually the best that money can buy. What we're spending on personnel security, by comparison, is peanuts. We hear of few, if any, instances of someone attempting or succeeding in gaining surreptitious entry to a SCIF. That doesn't mean that it isn't happening. However, we do hear of too many cases were individuals have compromised very sensitive classified information. Everything reasonably possible should be done to improve personnel security, including its timeliness, scope and quality. During our survey of Special Access Contracts, we observed several things in the personnel security area which, we believe, need attention. We plan to address these issues in more detail in the near future. I might add that DoD is equally concerned about personnel security. Earlier this year General Stilwell established a select panel of senior DoD officials to review the Department's Personnel Security Program, with the objective of determining if there are better ways of meeting security needs. The panel finished its study last month, and its recommendations are now under consideration. The major concern of contractors that we visited and of industry officials that we met at gatherings such as this, involves personnel secur-

ity — the paperwork, the delays, the passing and the transfer of clearances. We of the GAO, would be remiss if we did not attempt to add our support to needed improvements to the personnel security program.

I will close with a borrowed quotation from Abraham Lincoln, changing only the pronouns, because it sums up the approach to our work in the National Security Area. "We have always wanted to deal with everyone we meet candidly and honestly. If we have made any assertion not warranted by facts, and it is pointed out to us, we will withdraw it cheerfully."

U.S. DEFENSE POLICY, PROTECTION, AND THE FUTURE

General Richard G. Stilwell, USA (Ret.)
Deputy Under Secretary of Defense (Policy)
Department of Defense

It's a distinct privilege to be able to be here today because I know a little bit about the role that the National Classification Management Society plays in the overall security environment which is so important to our Nation. The only reason this old soldier is harnessed back to the government service is because he believes down deep in his heart that our republic faces and will continue to face in this decade the greatest challenges in its 200-plus years of existence. In addition to my duties with respect to matters of security, I do have some responsibility for the framing of the basic defense policies. They're classified, of course. At least they were until just a week ago yesterday when you could read the significant portions of the secret defense guidance in the pages of Aviation Week, even to the quotes, and then much of it today in the morning edition of The Washington Post. That simply points out to me the importance of what we're all about here, all of us collectively.

Part of our strength as a nation, as an alliance with our British and Canadian friends is the protection of our secrets, of our technological capabilities and of our plans.

The basis for our defense policies should be self-evident to us. They are our national objectives, which have extended virtually unaltered in the past three and a half decades since the end of World War II. They are pitted against the threats interposed to the attainment of those objectives; and most notably and most singularly the overall aims, the strategy for the attainment of those aims and the military power that undergirds that strategy, on the part of the Soviet Union. It's that half, the threat, which of course has constituted an extraordinary variable over these past two decades, and has changed the entire strategic environment. We must continue to remind ourselves that the attainment of our objectives as a Nation has just been rendered incredibly more difficult of accomplishment, of attainment, by the grand strategy of the Soviet Union and by the power that it has very studiously, methodically, relentlessly amassed to interpose its concept of future world order against our own.

This Administration headed by our great President has not changed national aims; it has not changed national strategy. It has however taken off the rose-colored glasses of the past Administration and, to a degree, the one immediately before that, and has realistically assessed the changes in the military balance which impose a need to revise certain of our policies to better deal with the realities in the world in which we must live.

In so doing, we have totaled up what we must contend with. We must contend with the Soviet Union who confronts us with a grand strategy of which its military power in only one component, albeit the indispensable component, because the only thing the Soviet Union can do well is produce military equipment and field military forces. Those forces are designed to undergird the political components of their strategy which in the end is targeted on extending Soviet influence without war, without getting Soviet bayonets bloodied except to the extent that may be necessary to complete the rape of Afghanistan. Also, to use its military overhang for purposes of coercion which have as its end purpose, zapping the vitality of our international free trade area; decoupling the United States from Western Europe, from the United Kingdom, from Japan; completing the encirclement of China; and gradually extending its influence indirectly to the areas on which all these industrial societies so heavily and utterly depend for the energy sources and the strategic minerals of the Middle East, Africa, and increasingly of Latin America.

In short, to follow the old Lenin dictum that the road to the West is there — Peiping and Calcutta, and by extrapolation to the Suez. That's where the jugular is, and at the end the game is not the overrunning of our societies but rather insuring that all major decisions — political, economic and the like, in the capitals of our free world — are based on the dictates of the Soviet Union, of Moscow and the politburo. And very significant among the tools being exploited by the Soviet Union to achieve that complex of aims, is that of misinformation, of propaganda, and the like, which bears a very, very great relevance to the anti-nuclear campaigns now rife, not only in Western Europe but increasingly in this country.

That is a threat. What are we doing about it? Well, in short, we're very serious about preparing for the exigency of war at both the higher and the lower level. This is necessary in order to insure against the outbreak of war and to insure that we can rule out force or the threat thereof as a major element in the international power competition; so that the United States and its allies can exploit our advantage in the non-violent dimensions of international competition — the political, psychologically, informational and other, where we have or should have the advantage. The important thing, and it's noteworthy — I should tell you that we have a Secretary of Defense who thinks in terms of the requirements for the conduct of war, which is our mission — *extremus,* and he does not stop his thought process at the terminus of deterrence. That's a very healthy sign. Because he appreciates, as the experience of our British colleagues in and around the Falklands now demonstrate, that the cost of one day of war is equal to about five hundred days of deterrence in both human and material terms.

The budget that's now under great scrutiny in our Congress is our translation of what it takes to field, equip, and sustain a very limited force during the coming year and those immediately thereafter in the light of its complex responsibilities, both to the defense of the United States and for the free world. It's a big budget, of course, but it cannot be looked at as something that is adjustable, maneuverable or changeable in the light of economic conditions. It's the cost in short of survival, and it represents a far less precentage of our national resources as was the case during Vietnam or Korea or any of the major crises of the United States' past history. The question, of course, is not whether we can afford it, but whether we can afford not to afford it.

My own synopsis of what's in that budget can be summarized in five basic thrusts. The first has to do with readdressing of the nuclear imbalance that exists today between the United States and the Soviet Union. The purpose of the President's five-point program announced last fall was to attain a U.S. nuclear posture which would deprive the Soviet of any incentive to use the threat of a first strike for purposes of coercion or influence on our decision-making process in time of crisis. This has to do with the strengthening of our command and control apparatus, the production and proper basing of the new intercontinental ballistic missile, development of a seaborne submarine-based counterpart, the purchase of a new bomber, and missiles to go with that bomber, and finally some enhancement of our strategic defenses, accelerated research and development with respect to anti-ballistic capability as well as a better capability to maintain the sovereignty of our airspace.

Now that whole program, of course, as you know has come under enormous fire and attention from the nuclear freeze, anti-nuclear movements that have swept this country in the last several months, and is still in my view unhappily growing momentum. It is fueled in part by the unwitting who are prey to the emotional appeals of people whose motives are certainly questionable, about the horrors of nuclear war. They forget that it's been the nuclear capability of the United States that in large measure is responsible for maintaining the peace for the last thirty years, that has permitted us to counterbalance the traditional overhang of the Soviet Union in land forces in the conventional means. They forget that today the nuclear weapons that we have and those that we have on the drafting board to produce as replacements are smaller, cleaner, and safer to handle than those in the past. The total implications indeed have gone quite the other way; and there's a suggestion in all of this, ladies and gentlemen, that if you could just get rid of nuclear weapons it would be a much safer world. There's a suggestion that somehow conventional war is acceptable and can be ration-

alized. Those of us who have been through one, two, and three wars know at first-hand that no war can be accepted with impunity. The aim has to be to have a posture which prevents, if at all possible, and type of conflict which involves the killing and maiming of personnel in uniform or out of uniform, if it can be avoided with honor and without sacrifice of any of the precious values and ideals to which we ascribe.

Well, anyhow, the *first* of those five points, of course, is the improvement of our nuclear posture, and the more so because for the Soviet Union, a measurable advantage and strategic nuclear capability would in its view give it almost unlimited scope for political coercive action around the world. The Soviet Union believes that although it's only one element of military power, it is the fulcrum on which all other power leaders depend. So that has to be our first claim, but a modest claim, and it represents less than 15 percent of our total resources. The rest are in the conventional area.

The *second* is the improvement of the ability of our forces, particularly those that constitute the strategic reserves in the United States, to respond globally to Soviet or Soviet surrogate challenges. The increasing power of the Soviet Union, increasing use of surrogates like Cuba, East Germany, and North Korea, and the improvement of its power projection capabilities means that it can confront us with crises in areas that were not possible ten or twenty years ago.

Moreover, we face the possibility, that over the next decade and more we can be confronted with concurrent crises in two or more areas of the world whereas our force structure has basically been designed in the past to deal with only one at a time. That means improved readiness for our forces — active and reserve — in the United States. It means very importantly an increase in our ability to deploy those forces to the far corners of the world if need be — such as the Middle East. This also translates into programs to increase the amount of strategic airlift as well as sealift as well as more positioning of supplies overseas, on land, or on ship and a great thrust to gain an additional access route for overflight for basing, for transit, in the various air and sea lanes of the world.

The *third* point, self-evident, has to do with our naval posture. A glance at any map drives home the point that our allies and ourselves constitute a maritime alliance, the individual members of which are dependent on free access to the oceans of this world for commerce in peace, for reinforcement, or for resupply in war.

The Soviet Navy has grown to the point where it can challenge our ability to control those vital sea lanes in periods of crises, as our own Navy and to a degree those of our Allies have attrited over the years. A major element of our defense policy is to increase the capability of the United States Navy to insure control of the sea lanes of communication as well as perform the other naval missions in time of peace or war as the case may be. It has also driven us, belatedly perhaps, into a hard examination of how better we might harness land-based facilities of other types to assist the guarding of those sea lanes of communication. In the role of land-based air, I must say, it has been demonstrated to a degree, unhappily, over the last several days.

A *fourth* element and a very, very important one is the recognition that in the new strategic environment, in sharp contrast to what has been the long strategy of the past, we cannot count on credibly threatening to escalate from conventional to nuclear combat in order to extricate ourselves from difficulty. Indeed in most instances one can envision it would simply not be in our interest to use nuclear weapons. That means that we can no longer take refuge in the concept of a short war, which was sort of a basic method of planning for NATO among others. Recognize now that if there is a confrontation with the Soviet Union, that conflict clearly will be indeterminate as to intensity, as to scope, or as to duration. This means in turn that we and our allies must have the same staying power as our adversary. That is clear.

What that means in turn is that we must have the capability to insure the support of our soldiers, sailors, airmen, and marines once combat starts from H-hour on D-day until the production base in the United States can begin turning out both the manpower and the material needed for combat.

There can be no break in that continuum; and this has resulted in, for the first time in two decades or more, some sincere honest tension and resources being devoted to mobilization, planning and preparations. As your corporations for the most part well know, the United States today cannot say that she is that responsible arsenal of democracy she was in two world wars before, unless and until we begin to fix things.

The *last* of these major thrusts, again, is that realistic assessment that in this age, this dangerous age, the concept of collective security has never been more vital. The United States can't, and shouldn't, try to do it alone. We need our allies and they need us; and thus one of our foci is to rebreathe the confidence of our allies in our resolve, in our intentions and to work with our allies to insure that together we orchestrate our respective capabilities and efforts to increase overall capabilities, to maintain the deterrent, or should that fail, to deal with aggression in a way that insures against its success.

Among other things this requires on the part of the leader — and the United States is the only nation that can lead this great free world today —patience, tolerance and understanding. Above all, it requires us, as is true of any team captain, to be out in front to set the example, to insure that we do no less than our full share, and to insure that we don't abandon the task even though sometimes there are problems with our efforts to get our allies to carry their equitable responsibility. Security assistance itself, military aid, training, and the like, loom large in that equation; and in this Administration the matter of security assistance to help our allies increase their defensive capability selfishly it suggests that there would be less need for U.S. direct support if the local concept has again been restored to its historic place as a major tool of the U.S. support policy.

This is the toughest of all of our jobs. It will be center stage in just a couple of weeks at the NATO summit where one can expect there will be some argumentation as to detail, but certainly a consensus that there is no alternative, for example, to the NATO alliance in its political, its economic and its military degrees.

Anyhow, those several thrusts are just one man's view of how to explain a defense policy of this Administration. It doesn't represent just throwing dollars at a problem. It does provide in our view a rational mix of conventional-nuclear-maritime active and reserve capabilities that add up to a policy which is equated to our times and gives prospective hope that the military shield will be adequate as the support behind the other instruments of U.S. national power on which we basically must depend if we are to block the further expansion of Soviet influence around this world and begin to reverse that. To the end that several years from now — maybe a decade, maybe two decades — certainly by the end of this great century, we will have brought about conditions which may force the Soviet Union to alter its grand strategy to become a more accommodating member of the international community and move us on that long, long road toward the development of an international community living under and being regulated by the rule of international law. It's a long hard struggle but nothing less than full appreciation of its dimensions and full commitment to whatever it costs, it seems to me, would square with our responsibility to our forebearers who have created this value system which is still the great hope of mankind. Anything less would not square with the responsibility that we have to our children and through them to their children.

I would conclude by again being reminded of something. A story told to me by one of my great heroes, of World War II, who as a young captain was aide-de-camp to the second chief of the Army Air Corps. The General had a penchant for going to a very famous seafood restaurant in Washington. He liked to go there on Fridays because he was a Catholic and he like to eat lobster. On this particular day he ordered broiled lobster. The platter was brought to him and he noticed the lobster had only one claw. He called the waiter over and said, "I want the rest of my ration." The waiter said, "Well, Sir, we try to keep these lobsters in that tank there so they're totally fresh for our customers and sometimes they fight and sometimes one loses a claw." The General pushed his platter toward the waiter and said, "Take this back and bring me a winner."

Well, you're all winners in my book by virtue of your membership in this Society, your dedication to the protection of the security of this United States of America and its allies. Your presence here clearly suggests that you also subscribe to what is really the secret weapon of the United States — the basic courage of its citizenry, the respect of all those things that constitute the American dream, and your determination that we'll do what we need to do to insure that they survive and prosper.

AN INFORMATION SECURITY OVERSIGHT OFFICE OVERVIEW OF EXECUTIVE ORDER 12356 AND ITS IMPLEMENTING DIRECTIVE

Steven Garfinkel, Director
Information Security Oversight Office

Let me tell you a little bit about the Information Security Oversight Office (ISOO) because there are so many folks here that I'm sure a number of you have no idea what ISOO is.

ISOO was established under the Order signed by President Carter in 1978 with the idea that there should be an oversight agency in the area of information security and President Reagan went along with that idea with a brand new Executive Order 12356, and ISOO as an oversight body will continue.

We have kind of an odd existence. For administrative purposes we're part of the General Services Administration (GSA), which obviously does not have a very major role in the security area outside the national archives function. But for policy purposes we don't take our directions from the Administrator of GSA but rather from the National Security Council (NSC).

In the past, we operated very autonomously. With the new Order, however, and with the interest of the NSC and the President in this matter, we have been operating very closely with the folks on the NSC staff and with Judge Clark, the Assistant to the President in National Security Affairs. What I would like to do is give you a little bit of a twist on this Order from my perspective as Director of the ISOO.

A couple of weeks ago I had the less than distinct pleasure of testifying before the Government Information Subcommittee of the House Government Operations Committee on the new Order. During the course of my testimony I introduced the Order with a short statement, and because that short statement includes the essence of what I think ISSO's major issue during the onset of the new Order will be, I would like to read that statement to you. Again, I was testifying before a subcommittee, so that will explain some of the language:

> Mr. Chairman, on behalf of the Administration I welcome the opportunity to appear before you today to answer your questions about Executive Order 12356 entitled National Security Information.
>
> President Reagan signed the Order on April 2, 1982, following many months of consideration. The Order becomes effective on August 1, 1982. In signing the Order, the President emphasized that its major purpose is to enhance protection for national security information without permitting excessive classification. He further states: "It is essential for our citizens to be informed about their Government's activities, but it is also essential to protect certain sensitive information when disclosure could harm the security of all our citizens. This Order established improved standards and procedures to achieve the proper balance between these two important objectives and permits the Government to classify only that information whose unauthorized disclosure could reasonably be expected to damage America's security. Limiting classification to the minimum necessary to protect the national security will enhance our ability to protect information that is properly classified."
>
> Mr. Chairman and members of the subcommittee, if I may, I would like to expound upon that last thought of the President's —"Limiting classification to the minimum necessary to protect the

> national security will enhance our ability to protect information that is properly classified." In making this point, the President is emphasizing the fact that it is critical to the viability of Executive Order 12356. An information security system is only as good as the classification decisions made under that system.
>
> If we violate the Order by indiscriminately classifying information that does not warrant this extraordinary protection, we jeopardize the information that does. As Director of the office responsibile to the President for overseeing his program throughout the Executive Branch of Government, that is the message that I and the members of my staff will be carrying with us, and that is basically the message that I'm carrying with me today.

We worked very hard to come up with a system that I think most of us in this room will think is an improvement on the system that existed previously — or a system that will exist from the first of August. The worst thing we can do quite frankly is to take advantage of those changes to the point of circumventing the kind of thought and consideration that is necessary in any classification process. There are more eyes on us right now with this new Order, and the purported changes and direction that it takes, than will ever be on anyone involved in information security.

They are all hoping that we will mess up, and if we do mess up, they're the ones that will turn out to be right. We're the ones who will turn out to have been wrong. So it's that message that I would like to impart here in the first part of my little talk.

The idea is that this Order was not created in order to classify more inmformation. It came about because of a perceived need to better protect the information that merits classification.. If it turns out that we are classifying and re-classifying and ignoring the mandates of the Order which limits classification, I think we'll see that this Order has a very, very short life span. Already, as you may be aware, there is some minor legislation that's been introduced to circumvent some of the provisions in the Order; and obviously the members, and the Chairman of the Subcommittee that I testified before were considering an entire information security system proposed by statute. This idea is something that every Administration — Republican and Democratic — has opposed from time immemorial. It is a position that I'm sure this Administration will oppose; but it is reality, and it becomes, far more of a reality if we make it so by failure to adhere to the requirements of the new system.

I would like to turn from that thought to the other direction, and that is the new Order's perception as a step backward. It's not a step backward, and I would like to talk about some things that I call media-myths. Obviously any time that you are going to seek to protect information in a better fashion, you're going to meet lots of criticism in the press. Quite frankly, I'm surprised that the crtitcism that we've received in the press over the last 6 months to a year, and most especially over the last couple of months, has been as moderate as it has been. I thought it would be much worse.

Nevertheless, there have been some things spread about in the press that I like to call media-myths. I would like to talk about them briefly today; and, again, this is not an overview of the new system at all. We could talk about the new Executive Order ad nauseam today, tomorrow, and on into the next national meeting. But by talking about a few of these media-myths, maybe I can touch upon some of the various interest that warrant your attention in order to understand just what it is that we intended to do with the new Order.

Myth #1. The Order will result in an appreciable increase in the amount of classified information. I find this is to be the most disturbing myth because largely it's an accumulation of the other myths that I'll talk about. The whole idea is that the purpose of the Order was to enable us to classify more and more information that does not warrant classification under the present system. Again, this is completely contrary to the intent of the changes that were made; and our oversight experience in the ISOO, and the statistical reporting that was gathered before ISOO came into existence, has indicated that the information security system in place, that

is, the Executive Order that bears on the classification of information, has relatively minor effect on the gross amount of information that is classified. We find that the most important variable is the state of world affairs; and, with the signing of EO 12065 and its total emphasis on non-classification and openness, the amount of information that was classified during its first year of operation was slightly down from the amount of information that was classified the year before.

But the following year when we faced the Iranian hostage crisis and the entire Iranian situation with the fall of the Shah, we discovered the amount of classification actually increased by about 10 percent; and, of course, this was at the time when there was the greatest emphasis within the Administration on security, and it appears from our observation that it was the state of world affairs that bore on the amount of classification.

From the best information that we have, and obviously it's not exact, in any given year there will be under a million decisions to classify information originally — somewhere between 800,000 and a million. That's a figure that we're going to be looking at in the next couple of years very, very closely, because if we discover that the amount of classified information increases appreciably, obviously our critics are going to say we told you so.

Of the systemic variables, of the things within the system that do bear on the amount of classification, one of them that is important, but again not nearly as important as the world situation, is the number of original classifiers. That variable seems to be the most important, and with the new Order we have attempted to limit the number of original classifiers to the number who were classifying information originally under the Carter Order. That's approximately 7,000 people worldwide. That's not a lot of people when you consider that about 10 years ago that number was close to 70,000 people.

The second myth is one more variable. Training is a definite variable, although perhaps not quite as important as the non-systemic variable — world affairs. Training is very important, and I think that's the reason that everyone is here today.

Myth #2. The Order requires when in doubt —classify. This is the myth that has gotten more media play than any other. You may be aware that under EO 12065 there is a provision that states (and I'm paraphrasing) when in doubt, leave it unclassified or at the lower level of classification. We have changed that from: when in doubt — classify, to when in doubt — find out. It seemed to us clearly irresponsible to make a decision one way or the other when you're in doubt. Why have a rule that must be applied 100 percent when there's not that must to prevent you from going to someone higher up in the chain of command, someone who has responsibility for these kinds of decisions, and getting a decision? We have made very clear that when you are in doubt, you have to find out within 30 days. During that 30-day period, you don't classify the information and then attempt to declassify it, if in fact you discover it should not have been classified in the first place. Rather, you don't mark it. You attach the appropriate memorandum to indicate that the information must be protected as if it were classified during this short interim period; and then at the end of that period, if necessary, apply the markings for classification.

Myth #3. By dropping the term "identifiable" from the standard of damage that is the threshold of classification, we have broadened the scope of classification under the Order. Those of you who are familiar with EO 12065 know that when we talk of the threshold of classification, we are talking about the Confidential level. That's the important level, contrary to its relative insignificance in terms of striking fear into your heart when we talk about Top Secret. Confidential is the level of about 70 percent of all classified information, and it is that level that is critical to the classification process.

Under EO 12065 it is stated "identifiable damage to the national security." Under EO 11652, the predecessor to EO 12065, it said "damage to the national security." Under the new Order it is again, "damage to the national security."

Why did we drop the word "identifiable"? Was its intent to broaden the scope of classification? No, not at all. "Identifiable" was applied to the standards for Confidential under EO 12065 in an effort to make clear to classifiers that they had to be conscious of the decision they were making,

that they had to think about damage. "Identifiable — think about it. Identify it in your mind —not on paper. There's never a requirement that you identify damage on paper, only in your mind.

Well, what happened was almost predictable. Those persons who sought access to classified information under the Freedom of Information Act (FOIA) and ended up in court, latched on to the word "identifiable" and said "identifiable" meant something more than damage to the national security. It meant a specific quality of damage or it meant a specific quantity of damage to the national security. This is clearly not the intent of the drafters of the Order, but it was argued in court. For example, there was a case decided a couple of years ago in which the requestors were trying to get some intelligence sources and methods for the CIA. They were before the Court of Appeals of the District of Columbia; and the plaintiffs, the persons seeking the information, argued that these sources and methods of information could not meet the standard of identifiable damage to the national security because it was merely speculative that there would ultimately be damage to these sources and methods if the information was revealed. Now, I think most of us would react to that by saying, "That's absurd." In other words, reveal who these sources are; and then we'll see if there's damage that results from that revelation. In this case, it may even have been the name of agents or something like that — I'm not certain.

That was the absurdity to which the term "identifiable" has been brought, and it was dropped because of this litigation problem. I might add —and this is very critical — that it does not mean that it is our intent that you should not bother to be conscious of the decisions you're making, to think about damage. That remains critical. When you get to court or when there is a request for access, a situation like that, you're still going to have to explain yourself. So it's better to explain yourself from the beginning, in your mind, so that later you may be able to explain yourself in that affidavit that you may have to submit before the judge.

Myth #4. The Order permits the classification of the telephone book, road maps, and annual corporate reports. This myth was the favorite of Representative English, the Chairman of the Subcommittee. He went on the national media frequently carrying phone books and said that they were going to classify these things. This is the most absurd of the myths. It results from a very narrow change in the Order, a change that is being read in a vacuum by its critics for purposes of making this public relations point, that is, that we have expanded the classification categories. In other words, of those categories of information that may be classified from seven to ten under the new Order —one of them, one of the changes, is a new classification category that pertains to the vulnerabilities and capabilities of systems plans, etc.

I might add that if I had had a totally free hand in redrafting the Order, the first thing I would have dropped would have been these classification categories. They're worthless. They were created under EO 12065 with the idea that if we create specific categories of information that may be classified, we have indicated that the classification process is limited. In creating the seven categories under EO 12065, with the inability to describe information with particularity —we have extraordinary broad categories — military plans, weapons, operations, economic, and technological matters pertaining to the national security — just about anything can be classified, just about anything!

Unfortunately, we failed to get a couple of things in these broad categories in EO 12065, and with the idea that we were going to continue classification categories because of the public relations aspect of the thing, of having a specific number of categories, we needed to increase it by a couple. One of them pertained to the vulnerabilities and capabilities of systems. It was a suggestion (I think originally from DoD if I'm not mistaken) and there is a case — Taylor versus the Army — in which it becomes a critical point. In that case that's now pending before the U.S. Court of Appeals, the reporter is requesting access to some readiness information of army units, or army units worldwide; and his argument is that readiness has

nothing to do with military plans, weapons and operations. The vulnerabilities and capabilities of systems would clearly encompass that kind of information, but it was added specifically to include some situations where we didn't have a clear category before.

For example, information pertaining to the protection of the President. That information needs to be classified; there is certain information that the Secret Service needs to classify. Information relating to civil preparedness. Oddly enough, we've failed in the other categories to include a category that would encompass civil preparedness information and information pertaining to the protection of our embassies overseas. Obviously, since 1978 we've recognized that that's a very important type of information.

To get back to the myth — the point raised by Representative English and others, is that by talking about the vulnerabilities and capabilities of systems, we can now classify phone books, corporate reports, things like that, all these big systems, all systems that arguably may sometime have some bearing on the national security. The fallacy is that there are really four tests before information can be classified, and Representative English is only looking at one of these — the question of whether information falls within a classification category. There are three others.

First, you have to have a decision made by an original classifier, and I talked earlier about the fact that there are a very limited number of people.

Second, you have to have information that the Government owns or controls. This is critical. The Government doesn't own the phone book. The Government doesn't own the annual reports of corporations. The Government must own or control the information before it may be classified.

Obviously the question of control is critical, but we (ISOO) do not want the fact that we possess information to equal control. We might have a copy of the phone book. We don't control the information that appears within it despite the fact that some of our critics have argued that possession is equal to control. It's not. Obviously if we either own it, or by some lawful arrangement, either by statute or lawful agreement, we control it, then we have the ability to release it, to withhold it, to transfer it, or to manipulate it generally.

And, last and most important, the information if disclosed must damage our national security. There are three other tests besides the classification category, but these were conveniently ignored in saying we were going to classify road maps.

And the last of the myths that I'm going to talk about today is that the Order forbids the classifier from considering the public interest in disclosure — the so-called balancing test that EO 12065 gives. Here, again, we're looking at a change to the Order in a vacuum when we say that.

For those of you who are not familiar with it, in EO 12065 there was a provision that said that even if information were properly classified, even if you could justify its classification, and if you had a request for declassification and release, the head of the agency in his or her discretion could weigh the public interest in disclosure — in other words, you could take a second look at the thing — and if it were determined that the public interest in disclosure outweighed the Government interest (and I might add the public interest in withholding) the information could be released notwithstanding its proper classification.

Again, this is not a problem with the concept. I think that concept is a very valid one. It's a concept that we apply every time we classify information and every time we declassify information or look at the information for declassification. What are the competing interest behind disclosure and protection? It is inherent in the process, but unfortunately the balancing test became the jurisdictional handle without peer in EO 12065 for litigation under the FOIA. The balancing test was applied or sought to be applied over and over again as a second guess to the role of the classifier; and we have proceeded to the point where we actually have some judges, who while previously reluctant to do so, are now willing to second guess on the question of whether information would damage the national security, notwithstanding their admitted lack of expertise in the particular subject matter area. And so the balancing test was removed not to take away our discretion to consider the competing interest but rather for us to avoid these problems in litigation.

I think I'll leave it right there, and if anyone has any questions I would be happy to entertain them on anything I've said or haven't said.

Question: In the hearing on May 5, the Subcommitte seemed to be very interested in the subject of reclassification. Would you like to address that, please?

Mr. Garfinkel: Certainly. What you are referring to is a change from EO 12065 to EO 12356. In EO 12065 there's a provision that says if information has been declassified and disclosed, it may never be reclassified.

During the course of our consideration of the new Executive Order, it came to our attention that there had been cases during the period of EO 12065 since 1978 where agencies had made mistakes. They had declassified information that probably should not have been declassified; they had released it to just one requestor, and realized their mistake subsequently. The information had not been further disclosed. The receiver of the information was willing to have the information retrieved by the Government. In other words, the requestor either wasn't that interested in that particular information or for some other reason was concerned about the security aspects as well.

But because of this provision, this rather inflexible position in EO 12065, the Government was unable to reclassify this information that clearly warranted it, and so we changed that in the new Executive Order to provide that under limited circumstances, the Government may reclassify information that has been declassified and disclosed.

I might add that this is a provision that concerns me a great deal, and it concerns me largely because of the potential for abuse. By pure chance, by pure coincidence, several cases involving the question of reclassification have arisen in this interim period between the signing of EO 12356 and its effective date in August. It has been pure coincidence, an unfortunate coincidence; but it leads us to understand that the potential for abuse is there, with the concept of reclassification. It is to that point that I testified to the Committee to indicate that our intent was really to take what is a closed door, the idea that you can never do it, and then to open it just a little bit of a crack.

Now how far that crack is open has one extraordinarily important variable, and that is the need to protect that information. How critical is that information? Obviously, if that information is extraordinarily critical to the nation security, we're going to open that door a little bit farther. I mean, we might open it to the point where civil litigation will be taken against the receiver of the information in order to try to retrieve it.

We hope to limit these cases to volunteerism. I can't say that I'm optimistic that that will always be the case. I would like to think it would, but I am sure that it won't; but the critical thing is that we're going to have to be very careful with that provision of the Order. We're going to have to oversee it very, very closely because it is the area of potential abuse that I don't see in most of the other changes that were made.

Question: What is being done on classification guidance and the downgrading and declassification problem. Has there been any resolution to that problem?

Mr. Garfinkel: I'm glad you brought that up because I should have mentioned it. I'll repeat it in a little bit different context. You're probably all familiar with the fact that GAO did a report about a year and a half ago in which they were critical of the classification guidance that contractors were receiving. In reaction to that, ISOO tried to go out on its own and confirm whether or not we thought the conclusions reached in the GAO report were correct, and to do that we sent our analysts to a number of different contractors in a number of difference areas — concentrated areas of large defense contractors basically — largely to look at the question of classification guidance and whether you were getting it and getting it promptly, getting it correctly, etc. We have all the data. That report should have been out and would have been out a long, long time ago if we had not we been preempted by the new classifications, the new Order. All of our resources to a large extent have been devoted to the question of getting out the new Order, and I have not been as concerned about not getting out that report because it remains a timely question.

We're trying to get out an implementing directive. We hope it will be out in early June. Once it's out, our first priority at the office is to get out this report on the question of the quality of guidance

that contractors will receive. We have all the data. We are aware of what our conclusions will be and hope to get out a decent report and get it to all of you.

One last item that I want you to be aware of. ISOO operates generally on a shoestring budget, but in the crazy world of budget situations today we had a little case of serendipity where we were presented with some money. Right about now we were told we had some money that we didn't know we had, but we couldn't hire any people. If we would find a nice contracting use for it, we could use this money; and what we are endeavoring to do is put together a couple of slide-tape presentations on the Order professionally done by contract with very quality-minded producers of this type of program. Our goal is to have this slide-tape presentation available before the new Order goes into effect. When we have copies of it, we're going to contact our agency liaison folks, all of the folks around Government.

It may be, of course, that some agencies will want to produce their own audiovisuals on the Order, and we encourage that. Obviously, ours are going to be generally geared, not specifically geared; we hope they will be available before the new Order is effective. We will have a general briefing on the system as a whole, plus two supplementary briefings — one on marking and one on safeguarding. I hope that they will be quality briefings and will be available for anyone's use when we have them produced.

DEVELOPING EFFECTIVE SECURITY INTERFACE TECHNIQUES WITH MANAGEMENT

Joseph D. Cooper
Manager of Security
Harris Corporation
Government Electronic Systems Division

The purpose of this presentation is to share with you some ideas about developing and maintaining management support for your security program. Although it is geared to Security Representatives in industry, I believe many of these ideas have applicability to Government Security Representatives as well. If you are expecting any new and startling revelations during the next 45 minutes, you are probably going to be disappointed. Instead, I am going to descibe some proven management techniques which can be applied to security. In most cases they should enhance security visibility and effectiveness within your organization. For simplicity I have divided the presentation into four topics:

1. Developing management support. It is never too late to start and the sooner the better.

2. Building the right staff. The right staff is even more important to the smaller security department.

3. Traits of an effective manager. Many ideas are common sense but may need reinforcing periodically.

4. Common mistakes made by security managers. These mistakes can really hurt the image of your department

Developing Management Support

In order to obtain management support, you need to develop a security philosophy compatible with the management style of the company. The security approach in a high production manufacturing environment where all employees punch-in at a time clock will differ greatly from a think-tank atmosphere where all employees hold advanced engineering degrees and have very few rules and regulations to restrict their creativity.

Once you have developed a compatible philosophy, look at cost-effective approaches that will meet Government requirements and your company's objectives. Some points to consider include:

1. Understand the role of security. Security is a service organization whose function is to assist management in implementing the security requirements that the company agreed to when it accepted classified Government contracts.

2. Understand your product or service. You can't recommend a security approach until you fully understand what you are trying to protect. Get involved technically so you can appreciate the problems associated with security implementation.

3. Determine management's attitute toward security. Through meetings and conversations find out management's perception of security and develop an approach that will clear up misconceptions about your role.

4. Establish priorities based on cost. Determine what is really necessary and what is nice to have. Do sufficient research or gather quotes to insure you know the true costs associated with a recommendation.

Once you have developed an approach, evaluate the effectiveness of the concept before implementation. Informally staff your approach with people who will be affected. They may be able to give you some good recommendations, and they will appreciate the fact that you discussed the plans with them first, and they will probably help you implement them successfully.

Now it's time to implement your approach.

1. Establish goals and review periodically. Be realistic and modify your goals based on changing events or circumstances. Don't push for an expansion in staff or equipment when the company is suffering a business slump.

2. Document your results. Ensure that management knows what you are accomplishing by submitting period or monthly activity reports. Be compatible with the present management reporting schedule.

3. Ensure that the basis for security regulations are understood. This is very difficult because the Government doesn't even know. Make an effort to understand the reasons behind security regulations, so you can explain and gain support for your approach to implementation. "Because it's in the Industrial Security Manual (ISM)" is not a good reason.

4. Participate in advance planning. Every major company has at least an annual operating plan, and some have 5- and 10-year plans. Explain your desire to participate so you too can plan ahead instead of reacting after the fact.

5. Be a team player. Let the people you support know that you want to help with problems so they will come to you before the problem gets out of control.

6. Develop a positive attitute toward security. If you have people working with you, your job becomes much easier.

Building The Right Staff

The greatest asset (or liability) you have to work with is your staff. Because it is people who create or solve problems, let's examine some ways to find people that can help solve your problems.

Before you start interviewing you need to do a careful profile on the position you want to fill. Work with your personnel department to establish a good job description if it is a new position. Make sure you know what duties and responsibilities you would like performed so that there are no misunderstandings after you have hired somebody. Next, establish an objective selection process that will match the "real" with the "ideal" candidate. It might be worthwhile to establish a point system to attach to desirable qualifications such as education, experience, maturity, etc.

Now it's time to start looking for the right person. Advertise in the logical places such as National Classification Management Society (NCMS) or American Society for Industrial Security (ASIS) and carefully screen resumes. Use the point system discussed earlier and narrow your field to the most qualified. If you have more qualified candidates than you wish to interview personally, use the telephone to weed out unqualified candidates. Develop a list of questions you would like answered based on the resume and your stated qualifications. After you have narrowed the field, bring the remaining candidates in for an interview. Because most supervisors hire based on emotion rather than rational choice, insure that you have other members of your department or company participate in the interview process and complete a written evaluation. This way, if problems occur later, they will have to share the responsibility.

Now that you have made your choice, do your best to insure that all available training and assist-

ance is given. If the person does not measure up to your expectations and will not fit in your department, make the hard decision and *do something about it*. Termination should be a last resort after you have tried counselling, attendance at training seminars to correct weaknesses, etc. Make sure you have everything properly documented.

Traits of an Effective Manager

The job of a supervisor is to guide, control, and direct the labor of subordinates. A study by the American Management Association found the following seven qualities evident to some degree in successful supervisors:

1. Knowledgeable in his field. There are several ways to accomplish this and all of you are obviously taking advantage of one — participation in this seminar. Other ways include college courses, correspondence courses, and attendance in NCMS Chapter meetings.

2. Efficiency oriented. This really means doing things better with the right combination of resources.

3. Logical thought process. Many people think this is a gift instead of a learned trait. It really involves the ability to assemble information, establish theories, then make decisions. All three can be learned.

4. Know where to get answers. Effective supervisors don't have to know everything, but they do need to know where to get the correct answers. Maintaining a reference library of regulations, procedures, and related books can supply the right answers

5. Develop subordinates. As you move up the ladder you will not be able to do all of the work yourself. Coach, counsel, and help your most valuable assets, so they can share in the workload

6. Communicate effectively. Make sure your subordinates know what you expect of them, and keep them informed of changes. Communication also means listening to others and encouraging ideas.

7. Manage the group. Get everybody working together. Avoid unnecessary meetings and praise cooperation.

Common Mistakes Made by Security Managers

These observations are based on personal experiences and are presented so that they will not be repeated as often in the future.

1. Avoiding the business aspects of the job. Learn budget preparation and live within your budget. Make sure you keep management informed of what you are doing by routine reports, etc.

2. Using "crisis management" in place of planning. This requires good coordination with management but will earn you the respect of top managers.

3. Presenting problems but no solutions. The natural impulse is to inform your boss the minute a problem arises. Try to think about some solutions before you give him the problem.

4. Playing favorites. Do not let your personal feelings cloud your judgment. Support everyone in the organization or the ones you don't will get you in trouble.

5. Blaming shortfalls on management. Never blame lack of management support for a deficiency uncovered during a security inspection. It reflects poorly on you and the company. If it was really important to you, you would have found a way to do it.

6. Allowing security to be used as a political tool. Be wary of others who try to use security for their own ends. This is not a recommended way to advance or to fulfill your security responsibilities. Security requires an objective and even-handed approach.

7. Allowing yourself to be pressured into a compromising position. If it happens once, you can bet it will happen again and with increasing frequency until you do not have a credible security program.

In summary, good business practice requires a stringent review of nonprofit-making activities. For this reason you already have management's attention. You should evaluate if that attention is producing positive or negative feelings and modify your approach accordingly. Simply stated, the key to good management support is *good management practice*.

COMMUNICATIONS SECURITY AND THE HUMAN INTELLIGENCE THREAT

Earl Clark
National Security Agency

Summary of Presentation

Mr. Clark, National Security Agency (NSA) addressed what many in the government consider to be one of the most serious security problems facing us today — The Cognizant Agent Threat —the cleared individual who for some reason comes under the control of a hostile intelligence organization, He then asked, "Why is it so important to protect our Communications Security Systems?" He noted that potential adversaries are interested in obtaining information on our sophisticated weapons systems and other highly classified programs. But, Communications Security Systems (COMSEC) are unique because they provide the protection for all our classified communications — if someone has access to our CRYPTO systems he can obtained information on all our critical secrets.

Turning to a point not always clear, Mr. Clark said that NSA is responsible for the design, development, and production of and doctrine for COMSEC systems for the Federal Government. However, he emphasized that COMSEC is a departmental responsibility and that each Government Department and Agency is responsible for managing its own COMSEC operations.

Regarding cryptography, Mr. Clark said that the United States has the finest cryptography in the world. Properly used we are confident that it protects our communications. He further explained that there are two basic elements that we must protect: the algorithm built into the hardware and the key used to set the equipment. Because equipments are in use for many years, we anticipate in design that at some point in their life span they may be lost. However, as long as we ensure the integrity of our keying material, these systems will still provide an acceptable level of security.

A prime objective is to preclude our equipment from falling into the hands of hostile intelligence for as long as possible. Mr. Clark emphasized that our equipments are often in development for many years before they are provided to our operational forces. Protection during this period is crucial and industry plays a very important role toward this objective.

Mr. Clark then addressed the Cognizant Agent Threat. Difficult questions in context included, "How does one ensure continuing loyalty? Are current tools in use today adequate?" Clearly, the United States must ensure the integrity of its Communications Security Systems. He noted that there is a myth regarding those cleared persons who are most likely to become Cognizant Agents — low-paid secretaries and low-grade enlisted personnel. Profiles reveal that grade, status or position are not true indicators of those persons who may betray their country. Profiles do reflect that money, ideology, and sex are prime reasons.

Mr. Clark went on to say that although recruiting of our personnel is a major concern, many of our most damaging cases have resulted from our own cleared personnel offering to provide classified information to hostile intelligence organizations. He emphasized that our personnel in the United States are just as vulnerable as personnel in overseas locations.

He discussed some of the actions currently under consideration by the Government that deal with the Cognizant Agent problem. They are:

- More rapid fielding of new COMSEC equipment.
- Reinstitution of the CRYPTO access requirements.
- Expanded use of the no-lone-access concept.
- Better training for COMSEC Custodians.
- Implementation of a Counter Intelligence (Non-Life Style) periodic polygraph for anyone

given access to cryptographic Logic of Key.

As an example of the problem. Mr. Clark provided some insight on the Helmlich case — the Army Warrant Officer who betrayed his country by providing highly sensitive and critical COMSEC information to the Soviet Union. Some of the highlights are:

- Mr. Helmlich's actions were self initiated. He was recruited by the Soviets.
- His role motivation was monetary.
- He operated for an extended period.
- There were many indicators in his lifestyle that should have caused the system to react. (Changes in behavior patters should be reported within the management. They need to be watched carefully and possibly be made subject to examination. In the Helmlich case, it was reported by a number of commanders that he lived far beyond his means. Unfortunately, the system didn't react.)
- When confronted. Mr. Helmlich refused to take a polygraph.

In conclusion, Mr. Clark stated that he could not forecast when the proposed policy and doctrinal requirements would be implemented. He was optimistic that it would be soon, as senior officials in government were very concerned about the problem and very supportive of efforts to take early and effective remedial action.

SECURITY EDUCATION — SOMETHING TO THINK ABOUT

Joseph A. Grau
Security Education and Training Specialist
Counterintelligence Directorate
Office of the Assistant Chief of Staff for Intelligence
Department of the Army

What I'm going to be talking about today is not security. It's security education, and there's a big difference. Before I forget, let me make the standard disclaimer that's required of all good bureaucrats. My remarks here today do not reflect the official position of the Department of the Army or of Defense or of anyone else. They're my thoughts and my opinions and my conclusions based on a year and a half of taking a good hard look at security education.

In October 1980 I moved into a newly created position on the Army staff as the principal action officer for security education and training. The mandate was to do something to improve security education within the Army. The first task, as I saw it, was to find out just what the state of the art was out there in the real world as opposed to our view of it up there in the five-sided puzzle palace.

For the past year and a half I have spent a lot of time on the road, visited 13 Army major commands in the States and overseas and some 15 other Army units and organizations. I've also done a lot of talking with folks like you — security professionals from other Government agencies and from industry — about security education. What I'm going to do today is try to give you a bit of the benefit of what I've seen and what I've heard during the past 18 months. Now these observations are primarily what I've seen within the Army, but I think I've seen enough of what other folks are doing to be confident that they apply throughout the security community.

Let me start with a definition, even though I hate people who start with definitions. What is security education? To me security education encompasses everything we do to provide our people with information about security policies, procedures, and practices — and everything we do to either reinforce or change the ways they behave so that this behavior is supportive of our security programs. You'll notice from this that we have to do a lot more than warn people and scare them about the espionage threat, and we have to do a lot more than teach hard skills.

Before we get into what security education is like now — the current state of the art — let me share with you my perceptions of a pipe dream, what the program should be like, the requirements for a viable program. As I see it, there are four basic requirements for components of a good security education program. You have to have all four of them in your program if your program is

going to be effective and if you're going to satisfy the requirements of the various regulations and directives we operate under.

Individual presentations — and please notice the distinction I make between presentation which is what I'm doing now and programs which is the totality of your security education effort. The individual presentations you usually find tailored very heavily towards one or two components. There's absolutely nothing wrong with that. The problem is too often an entire program in an organization is heavily weighted to one or two, which means that something else is neglected. We need to look first at what the individual components are, realizing that there are fine lines — gray areas — between them. And we'll look at them from the point of view of the effect that they are intended to produce in an audience.

First of all, awareness. We want to have people acknowledge the existence of a threat. We want to instill an awareness that the espionage threat is real and can be faced by any of us anytime. A lot of us who have been in the security business for a while find it awfully hard to believe. And especially after all of the publicity we've seen about Boise and Campalis and Helmick and Belzacarsky, there are still people out there who don't realize, don't admit to themselves that espionage is for real and that they themselves can be caught up in it anytime. We want them to be aware of ways in which hostile espionage services operate so they can be alert to situations where they might be affected, so they can understand the need for the good security practices that we're going to require of them.

The second component is motivation. We want the audience to have a desire to apply good security practices, not just some kind of a vague hope that the Russians won't get us or espionage won't succeed; we want a positive desire to have good security, a desire that's strong enough to motivate them to take action.

We must also concern ourselves with education. We want to produce a good, solid understanding of the basic policies, the basic principles of the information security program and related programs. I'm not talking about skills — hands-on, doing tasks, I'm talking about a knowledge of the policies, the procedures, the philosophies, that make the skills necessary and meaningful. This is related to the very basic, very proven principle that you're going to do a better job of something if you know not only how to do it but also why you're doing it.

Now, of course, you can overdo this. You can spend so much time on highfalutin philosophy that you never get around to teaching the basic skills. You can shoot way over the heads of an audience and put them sound asleep. And unless you make it very clear why they should be concerned with these policies and these philosophies, you can bore them into a near coma. But the advantages of having people applying security procedures intelligently, giving you decent feedback on the effectiveness of the practices that you expect of them, are very important.

Finally, we have training which is probably what we do the most. We want to teach the skills needed for actual hands-on running of the program — everything from how to mark a classified document to how to apply classification guidance, to how to adjudicate a security clearance determination, to how to report espionage contact.

We need to include each of these components in our program. and we need to do something more. We need to make very certain that the programs we present are suitable to our audiences, to tailor the programs to meet the needs of the people we're talking to. It's just common sense that different people with different duties and responsibilities need to know different things about our security programs. That's what we need to do.

We need to make certain our program effectively includes *awareness* and *motivation* and *education* and *training*. We need to make sure it's well tailored to suit the needs of our audience. And it goes without saying (but I'll say it anyway) that our programs need to be high-quality efforts. In any educational effort, a shoddy presentation gets shoddy results.

Now let's look at the real world. What is security education really like today? First of all, let me tell you I really believe we've seen a genuine increase in emphasis on security education over the past couple of years. People and organizations who

were rather lackadaisical about security education in the past seem to have realized that the program is important and that it does need emphasis. We see resources committed to security education in organizations where it's never happened before, and we see people trying hard. That's encouraging, but how well are we really doing?

In my opinion, we're been doing a pretty good job for a number of years in the awareness phase of the effort — not perfect, mind you. There's room for improvement as there always is. We haven't been doing too bad a job in motivation either except for a problem of misplaced emphasis that I'll get back to in just a while. We've also been teaching skills, maybe not always as well as we should, not always to everyone who needs them, but we've been trying. In my opinion, this leaves one area where we've all been falling flat on our faces and that's *education*.

We pay attention to education once every few years when we get a new Executive Order; and then we gear up, and we all wax eloquent on the "new philosophy of classification in the Order," which usually turns out to be not really so new after all, just a change of emphasis or means of application. Then that's it until a new Executive Order hits the streets.

We're doing awareness programs because there's some good canned material available, and some of us have access to folks who will come in and do them for us which makes things very easy. We're attempting motivation because, as we'll see in a moment, we've found an easy way out there too. We're teaching skills because high levels of skill make us pass inspection. And we ignore the education component because it's very difficult to do well and because we don't see direct, immediate benefits from it.

Don't get me wrong. We're not doing this deliberately. We're doing it because our time and our resources are limited, and we naturally tend to concentrate on aspects of the program where we see high payoff, and where we can do them with minimum resource expenditure.

How about tailoring, suitability, audience specificity? Well, unfortunately in the real world, we find the infamous annual security briefing — a security office's once-a-year monumental effort to get security education out of the way for the year. So the great day arrives and the first of the program starts in the biggest auditorium on the installation.

Now I say the first of the programs because the auditorium only holds 200 people and there are 2,000 people in the activity, which means someone is going to present the same program ten times. And the audience files in, everybody from the deputy commanding general to the young man who maintains drivers' records in the motor pool and has never seen a piece of classified information in his entire life. In case you think this is unusual and just happened this one time, if you go to the other nine presentations, you'll find about the same mix of people. What's wrong with that?

What's wrong is you're just about guaranteeing that you're going to lose a good percentage of your audience in every performance. As far as level of understanding goes, you've guaranteed that you're going to be shooting right over the heads of some people and insulting other people's intelligence. You've also guaranteed that you're going to be telling some people a lot more than they every needed or wanted to know about some subjects while leaving out or brushing over something they really needed to hear about in more detail.

Some examples: The deputy commanding general. He doesn't really need to know all the details and the technicalities of how to portion mark documents. He needs to know that the requirement exists and generally how the system operates, so he can be alert when he signs or approves a document to see that it is portion marked and it looks correct to him. On the other hand, he might have a real need for good, substantive information on original classification and how he goes about making those decisions.

For his secretary, the situation might be just the reverse. She needs to be intimately familiar with portion marking details, but it's obviously not so important for her to be well versed in the process of original classification. Of course, both these people need awareness and motivation presentations, but it's also obvious that different approaches to these subjects would be appropriate because of their different lifestyles, responsibilities, and the

rather subtlely different threats that they're going to face.

And do you remember the young man from the motor pool — the one who has never seen a clasified document? What earthly purpose could it possibly serve to make him sit through a lecture on portion marking or on how to classify information? He needs to attend a good awareness and motivation program tailored to his need to realize that even though he has access to nothing that is classified, he might well become the target of a recruitment effort by a hostile intelligence service. He needs to know how this might happen and why. And he needs to know what to do if he finds himself in such a predicament. He does need to understand what classified information is and why it's important to protect it in case he finds himself involved in some sort of security violation, for instance, somebody walking up and handing him a CONFIDENTIAL document. And that's all he needs to know.

The next question is, why not teach him all this stuff about classification and portion marking and so forth? He might have use for it some day. What could it hurt? The danger is that we're dealing with logical, intelligent people no matter what their position in our organizations. The danger is that he's going to realize that much of the information you're giving him doesn't mean anything to him and isn't applicable to him. He's going to logically assume that the whole program is meaningless for him. He's wrong. but that's human nature.

Now the shotgun approach I've just described isn't universal. I've seen some well-tailored programs. But the shotgun approach is entirely too common. And wherever we find it, we find security people wasting their time and their audience's time and leaving unfortunate bad tastes in the mouths of people whose cooperation we all really need.

How about quality? How good are our security education programs technically? Are presentations put together and delivered effectively? Are our materials of professional quality? The answers to these questions range from terrific to horrible, from outstanding to appalling. I've seen security education presentations that were top shelf, truly professional products; and I've seen others that I could not show to my six-year-old son without pangs of conscience.

Now I've told you what's wrong, told you the negative. Let's take a look at some of the causes of these problems that I've just mentioned. Let's get the most often heard problem out of the way first; and it's a real problem — lack of resources. As in everything else we do, we don't have the people, we don't have the time, we don't have the money to do everything we want to in security education. To whittle down this problem, we need to do two things.

First, like anything else we do that expends resources, you have to convince the boss, whoever he is — the guy who doles out the resources — that there's a payoff, that security education is the least-cost solution to a problem. Try an old cliche — an ounce of prevention is worth a pound of cure. Security education is compromise prevention. What costs more? accident prevention or law suits and high insurance rates? fire prevention or replacing buildings security education or compromise investigations, criticism and embarrassment because of poor security, and damage to our national security?

The other thing we need to do is make sure that we expend these scarce resources that we have in absolutely the most cost-effective way. And we'll be talking about a couple of ways that we can think about doing this a little bit later.

Now there are other problems too. It's my experience that people in the security business are security experts, not educators. I've encountered any number of highly professional, competent, experienced security specialists who don't have the foggiest notion of how to put together a good security education program. This is unfortunate, but it's quite understandable. So what do we do about it? How do we become security educational experts, or at least as close as we can reasonably hope to get?

Basically, we keep our eyes and our ears open. Watch how other people do things well and learn from their mistakes. Ask questions about how a good presentation was put together, how a good

piece of material was developed. Keep your eyes open for the tricks of the trade. Talk to other people who do security education.

When I talk to somebody about security education (and I'm as guilty of this as anyone else) we talk about materials. We talk about sharing stuff —a film, a tape, a handout, a brochure, a handbook. We don't talk about ideas. We need to talk about ideas, programs, plans.

Another problem, also understandable but less excusable, is that there are a lot of folks out there who are waiting for somebody else to do their jobs for them. With limited resources and a nagging feeling that they don't really know enough to go about putting together a good security education program, it's a great temptation for security folks in the field to wait for higher echelons of command (or in the case of industry — corporate headquarters or the Defense Investigative Service) to spoonfeed them programs.

Let me tell you right now, I can just about guarantee that this is the case in the Department of the Army; and I hope it's the case in other agencies, that if common sense prevails, this is never going to happen. The higher up the chain of command, the chain of management, you go for programs and canned presentations, the less-specific, the less-tailored, the less-meaningful to your particular audiences the programs necessarily become. Higher levels of management in Government or in industry should provide guidance, suggestions, support, material, and ideas. The programs, the presentations themselves have to be put together where the rubber hits the road--by the security people on the scene in the activity. This is the only way they can be suitably tailored toward their target population.

Enough for generalities, enough for philosophy. Let's get down to some specifics, some things we should be thinking about. Let's look first at this motivation component of the program that I mentioned earlier. I mentioned a problem of misplaced emphasis, but just what is the problem?

We've got two types of motivation we can employ. You're all familiar with them, whether you're familiar with the terms or not — negative or positive. Negative motivation is a threat, the threat of some sort of punishment or some sort of unpleasant experience for doing something or failing to do it. In our context, it's the threat of criminal prosecution for willfully compromising classified information or administrative penalties or embarrassment at least for failing to follow security procedures and regulations.

Positive motivation involves the promise of a reward, either tangible or intangible. In the security field, the tangible rewards are few and far between. In fact, I would be hard pressed to give you an example. So we're forced to rely on intangible rewards — pride in a job well done, the satisfaction of contributing to the national security, things like that.

In my view, we misplace our emphasis by overdoing negative motivation in our security education programs. Why? Because it's easy. Negative motivation is quick and easy. We reel off a few horror stories about poor folks who have been disciplined for some sort of gross violations of security regs, we tell a couple of exciting spy yarns and read a few paragraphs from Title 18 of the U.S. Code, and we think we've done our job. But there are some problems.

First, you can't help wondering if it does much good. People who commit espionage, who deliberately compromise classified information know it's illegal. Everybody knows it's illegal, but they still do it. People who violate security regulations most often do it out of carelessness, ignorance, just like they violate other regulations. And threats of punishment don't seem to be of much use in overcoming this expediency or stupidity

We also have to be very careful of its negative effect. In the security business we need to have the fullest possible cooperation from everybody in our organization. You can't go around trying to win popularity contests, but we have to avoid developing adversary relationships with management and our co-workers. Willing cooperation is the best atmosphere we can engender to promote good security programs. Constant harping on penalties, on laws, on prosecution can leave the impression that the security people's goal is to play "gotcha" with their fellow workers.

Finally, it can be dangerous. In cases of security violations and compromises, knowing the exact circumstances surrounding the incident and knowing quickly is often vitally important. Overemphasis on penalties, on prosecution, on punishment can hamper our efforts to find out exactly what information might have been compromised, just what happened, or even that anything happened at all. Generating an atmosphere of fear generates an atmosphere of coverup, paticularly dangerous in our business.

Don't get me wrong. I'm not suggesting we ignore negative motivation. It's an important psychological tool. We need to take advantage of it. But we need to have balance. We need to appeal to a person's patriotism, his sense of responsibility, his good sense, and his desire to do the job right.

Now let's look at tailoring. Why don't we carefully tailor all of our presentations to specific audiences?. We can agree that they ought to be designed specifically for each audience we face so that the people are getting the information, hearing what they need to hear specifically.

The first reaction is almost certainly, "That sounds great. Give me another 20 people and I"ll be glad to do it." I'm talking about perfection and nobody's perfect, but I'd like to suggest an approach to you that can help us get a lot closer to perfection than we usually get today, maybe without too much greater cost in time and effort.

The major problem seems to be that we can't devote sufficient time and effort to preparing separate programs for every type of audience we face. It's not the problem of presentation. We usually don't have the facilities to present one program and cover everybody anyway. It's in presentation time that our problem comes up. It's obvious that putting together ten programs for ten different audiences segregated according to the type of program they really need to hear, is going to take ten times the time and effort that putting together a single general-purpose program would take. It is obvious but not true. It's going to take some extra work, but if we use the type of approach, the type of thinking about the problem that I'm going to suggest, it probably is not nearly as much extra work as we might imagine.

The problem is one of viewpoint. We look at presentations as single units, monolithic lumps, indivisible wholes. We work on the entire presentation, and we only have time to do one or maybe two and certainly not ten, as we would need for ten different audience groupings. I would suggest that we approach security education as a modular activity with what I call the modular approach, a system of putting together tailored security education presentations.

Step one — analyze your audience. Figure out what types of people you need to educate based on duties, responsibilities, and their type of interaction with the security program. Make your category specific but be realistic. A list for an activity might be something like this: top management, middle management, action officers, engineers scientists, clerical people, guards, computer operators and programmers, maintenance and service people, and communicators.

Step two — identify topics. Take a good hard common-sense look at what information you need to get across. Look at the four components of the program. Use them as sort of a spare outline. Look at inspection reports, newsletters, regulations, other people's programs, anywhere good ideas might be hidden. Now at this point, don't be too selective. Jot down all of the items, all the topics you think of.

Step three — match the topics you've come up with to the audiences you've identified according to what categories of people need to hear about what. This is the start of tailoring. You're probably going to find out that some of these topics are appropriate for everyone; others may be appropriate for only one or two groups.

Step four — allocate time. You've got a sketchy outline for each audience. Now you have to make careful judgements about how much time you should devote to each topic in each presentation. You're going to have to whittle down your list of topics. You're almost sure to find that you can't cover everything in the time available.

Step five — hunt for materials. (It's important to notice that we've gone through four steps before we get here.) Scour every source you can find for

good audio-visual material, artwork, outlines, programs done by somebody else that you can plagiarize, whatever. You know where the sources are. You can find the material. And while you're doing this, don't forget to check your own file cabinet for the oldies but goodies. You know, you did a program ten years ago at some other installation. There still may be some good material that would be fresh to the audiences that you're going to face now.

Now comes the modular part. Make up your presentations in modules. Don't try to put together a one-hour security briefing. Put together small segments of it — a 10-minute video tape on telephone security, a 15-minute slide lecture on NATO documents, a 15-minute practical exercise on portion marking, and a 20-minute film on hostile intelligence methods. Make up your modules according to the topics that you've identified for particular audiences.

Finally, take these modules and combine them into presentations. Fit them into the sketchy outlines you have for each audience. You may find that some of your presentations now are complete. You've filled them all with these modules. For others you're going to have to do some bridging and some introductory material. In some you're going to have large gaps, and you're going to have to prepare material to fill them. When you write this material, also do it in modules. You're going to find at this point that several or most of these modules that you've prepared are suitable for almost all audiences that you're going to have to face, with just a few words changed to fit a particular group. And that's it.

What you've got now is flexibility. When you have these modules prepared, you can mix and match them into an absolutely mind-boggling number of presentations — long ones, short ones, presentations for all sorts of audiences, tailored presentations suitable for all audiences. You're probably even going to have a few unused modules left over that you can save for the next time. Put them in your oldies but goodies file, you can use one-year-old material instead of ten-year old material. That's the approach.

I'm not saying that this is what you're going to do when your boss walks in and says, "We haven't had a security education program for a year." What I'm suggesting is that we can use this line of thought when we think about security education all year long. When you find a piece of good material, you can think of it as, "There's a perfect module to use in next year's presentation;" but you should think of it as a module on a particular topic that you can now match to an audience rather than a piece of material that you can use in a presentation.

Let's get a little more specific. Let me talk to you for a few minutes about one very common security education technique that will give you an idea of the kind of thinking we need to be doing about the material that we use. Let me talk about audio-visual material, particularly video tapes and films.

I've got two questions for you. I don't need an answer. First: How many security education presentations have you ever given or ever intended to give that didn't include at least one tape or film? Question number two: Why?

The answer to Why? is because we're brainwashed. You can't talk to anybody about security education for more than five minutes without his asking if you have a good tape he can use —with a hungry gleam in his eye while he asks you. We're brainwashed into thinking we have to have a video tape, we have to have a film in every program we do or somehow the program's not complete. This is nonsense, but it's persistent nonsense. We badly need to take a good look at how we use tapes and films, their advantages and their disadvantages. As a positive note — let's look at the advantages.

First of all, tapes and films make things easy, especially if somebody else does them for you. Quite a number of films and video tapes have been prepared by various agencies and various departments; some have been very good. People are usually quite willing to share them, and they take up 15- to 20-minutes of that great hour of our security education presentation. Films and tapes can also be very cost effective, especially when you have tighter constraints on manhours than on money. They're also very consistent. When you get a good presentation on tape, you don't have to worry about the speaker having a bad day or getting mixed up in the middle of his script, or having a cold, laryngitis, et cetera. You're sure that the

presentation is going to include exactly what it should everytime it's given. They can also increase retention dramatically. I've heard the figure of 400 percent when you mix sight and sound over one medium or the other. And, of course, you can do many neat things with films, tapes, animation situations, et cetera. But what are the disadvantages?

First of all — this is extremely important — if you're going to use tapes and films today, particularly video tapes, you'd better do a really good job of it. Television has made people extremely sophisticated when it comes to what they see on that little screen on that little box. If you show them a low-quality, low-budget presentation, they're going to realize it's low quality; they're going to realize it's low budget; and they're going to make the connection that what you're showing them isn't really very important after all or there would have been more resources put into it.

You also have to make sure that you make the tape a grabber, that you introduce it properly. There are a lot of folks that when you say, "Now we're going to show you a film," that's their signal for a short snooze. The lights go down and so do the eyelids. If you have a presentation that's tedius when somebody's up here doing it live, people at least have the excitement of wondering whether he's going to get lost as he goes down the page; but when you put that on tape, it's going to put them to sleep.

Also, audio-visual products unfortunately lack self-destruct mechanisms. In 1975 I attended a security education program which featured a film made in 1958. I invite you all to imagine the reaction of the audience when President Dwight D. Eisenhower introduced the film. There was nothing wrong with the film or with what it said. The information in it was still current, still valid, still important; but you couldn't convince anybody in that audience of that. You are insulting them by making them sit through an old film.

And if you really want a problem, and if you really want to turn off a roomful of people, get yourself one of those old films. Show it, and then stand up in front of them and say, "You saw in the film where you put the classification markings at the end of the paragraph. That's changed now, and you put it at the front." Then recite a list of requirements that have changed.

The last problem we have is that films and tapes are not specifically geared to the individual audiences that view them. To give you an example, the Defense Intelligence Agency (DIA) puts out a lot of good tapes. They're generous about sharing them. A lot of Army activities have found out about this. Bless their hearts! They write to my office, and they ask me to get them some. I had a dental detachment at an unnamed Army installation who asked me for a copy of "The Spies of Washington." They are at least 2,000 miles from Washington.

I've got a nightmare, folks; and in this nightmare an elderly gentleman, who drives a forklift at an Army depot in the midwest, is forced to sit through a video tape on access control procedures at DIA headquarters. You're all laughing, but we sent just such a tape to an Army depot in the midwest a couple of years ago.

Be prepared to discover that when you get ahold of these tapes that sound so good on paper, they don't mean a thing to your audience. And never, never show a video tape or show a film without looking at it yourself first. Don't construct presentations of one medium, be it lectures, video tapes, or whatever. Audio-visual products give you the perfect way to put some variety into presentations. That's what you ought to be using them for.

I've sat through presentations where you'd see a 20-minute video tape. Then you would hear, "Now we're going to show you a video tape on such-and-such," and you'd see another 20-minute video tape. At the end of that when your patience was exhausted, you'd hear, "Now we're going to show you a video tape on such-and-such," and you'd sit through another one. Barbara Mandrel or Hill Street Blues" might be able to keep our attention for a full hour, but I guarantee you our security education tapes can't do it.

Also, one last hint. Don't get into the habit of saving your video tapes or your films for the last thing on a program. Like I said before, video tapes and films can be the signal to some folks for a snooze. If you show them after your audience has been sitting there in a hot room for an hour, you're

sure to put them sound asleep.

As I said before, I'm a little short on time. The rest of that stuff on the handy-dandy outline that you have in front of you will be in the Journal. I know that I've violated at least eight or nine of the trainer's ten commandments today, particularly "thou shalt not preach at your audience interminably. Thou shalt not try to give a presentation without an armful of razzle-dazzle visual aids. And thou shalt not open every presentation with a horrible joke." Let me give you just one more piece of food for thought. You're going to hear a lot of folks tell you you need to do more in security education, and I can't argue with that. But I'm telling you that I don't particularly care, in my case, about Army folks doing more in security education. What I care about is that we do it better. And the key to doing things better is thinking hard about the type of subjects that we've just had a chance to touch on today — balance, tailoring of programs to audiences, and how to best use the tools and the techniques that we have available. Also when new people in the agency see three stars on a shoulder and the man's telling them, "This is an important subject, you should pay attention," that is a grabber. If you can get your boss, the head of the agency, to give you five minutes of his time to make a few personal remarks to the audience at the start of the program, that's a super way to make sure you've got their attention. If not, try one of these tapes. Just some short remarks, nothing substantive, just to let the people know that management is involved with the program, particularly if you've got a program that's a little controversial or that sounds new. What I think of right away is OPSEC, which I know a lot of the people in industry are getting involved in. This is a good way to show that management supports a new or a revised program.

SECURITY EDUCATION — SOMETHING TO THINK ABOUT"

Definition of security education: Every thing we do to provide information about security policies, procedures and practices, and everything we do to modify or reinforce behavior so that it is supportive of security programs.

Requirements

Program components:

Awareness: Acknowledgement of the existence of the hostile intelligence threat and understanding of hostile intelligence methodology.

Motivation: Desire to apply good security practices.

Education: Solid understanding of security policies and principles.

Training: Skills required for program implementation.

Tailoring

State-Of The-Art

Increase in emphasis

Program components

Tailoring

Program quality

Causes of shortfalls:

Lack of resources

Lack of expertise

Waiting for someone else to do the job

Methods and Techniques

Positive vs. negative motivation

Tailoring and a modular approach:

1. Analyse your audience
2. Identify topics

3. Match topics to audiences
4. Allocate time
5. Hunt materials
6. Prepare presentation modules
7. Combine modules into presentations

Videotapes and films

Advantages:

Easy

Cost-effective

Consistent

Enhance retention

Technically flexible

Disadvantages:

Require professional production quality

Can lose audience

No self-destruct mechanisms

Not specific to an audience

Hints:

Mix your media

Don't put tapes or films at the end of a program

Posters

Purpose

Techniques for attention-getting:

Size and design

Use of cartoons

Frequent change

Presentation techniques:

Management involvement

Audience involvement

Handouts

SECURITY EDUCATION IS COMPROMISE PREVENTION

PROTECTION OF THE SPACE TRANSPORTATION SYSTEM (STS)

Kenneth E. Lopez
Director of Security
Kennedy Space Center
National Aeronautics and Space Administration

Summary of Presentation

Kenneth Lopez, National Aeronautics and Space Administration (NASA), Kennedy Space Center (KSC), Florida, presented an overview of the Space Shuttle Program that included Shuttle Processing, Mission Profiles, and the Security Program.

He explained that NASA's Space Shuttle is being developed as a reusable system for transporting people, spacecraft, and equipment to and from earth orbit at a fraction of the cost of expendable vehicles. In addition to launching unmanned satellites, the Shuttle will permit their retrieval or even repair in orbit. Its versatility and reusability will allow the Space Shuttle to significantly reduce the cost of space missions and will open the benefits of space technology to people everywhere. The Space Shuttle opens a new era in the exploration and utilization of the space environment.

Unique Security Program

Mr. Lopez stated that NASA has some unique security programs designed to provide essential safeguards for this great national resource. He explained that the NASA Security Office is responsible for developing and managing the Government security, and for coordinating intelligence and law enforcement programs at the Space Center. The Security Office has a Civil Service staff of 16 people who oversee a broad spectrum of pro-

grams, including information, personal, physical, technical, communications, industrial and launch operations security.

At this time, the staff is supplemented by a protective services contractor, Wachenhut Services. The contractor is responsible for planning Shuttle security, maintaining security systems, and general law enforcement tasks such as traffic and crowd control, access control, facilities protection and emergency response.

STS: A Vital National Resource

Security operations in support of the STS fall into the following categories: protection of high priority national resources, protection of classified payloads, and security for safety reasons.

In 1978 a Presidential Directive declared the STS a vital national resource. The National Resource Protective Program (NRP) requires that extraordinary protective measures be instituted to safeguard this one-of-a-kind national asset. At the Space Center the NRP program has three elements of protection: an Alert Team, Target Hardening of Facilities, and Sensor Sophistications for air, water and ground threats. Four million dollars has been earmarked for security enhancement under the NRP at the Space Center.

Mr. Lopez stated that over 40 percent of all Shuttle flights will have classified military payloads. Classified payloads are not new to NASA; however, the magnitude of these missions will change their operations and require extensive NASA coordination with the Department of Defense.

Personnel Reliability Program

Personnel security requirements are of extreme importance to the STS program. A Government investigation is required for access to all Restricted Areas. Security clearances are required for contractor and government employees

Additionally, a Personnel Relability Program (PRP) is used for screening employees that require access to mission critical hardware assets and operations. The PRP assesses employees for their ability to make critical value judgements; it also assesses their technical ability to perform mission critical duties and their medical fitness, as well as assessing whether they have favorable backgrounds. An additional purpose of the PRP is to determine if an employee might pose an international threat by harming or compromising hardware, operations or information, or an unintentional threat by exercising poor judgement caused by fatigue, alcohol, or drug abuse.

Mr. Lopez gave an excellent and interesting presentation on the complexities of the KCK Security program for the Space Transportation System.

This summary has only touched the surface and highlighted some of the functions of a very complex security program.

REMARKS ON THE BALLISTIC MISSILE DEFENSE OPERATIONS SECURITY PROGRAM

Elmer F. Hargis
Ballistic Missile Defense Systems Command

I really appreciate the opportunity to talk with you on Operations Security (OPSEC) in the Ballistic Missile Defense (BMD) Program. Figure 1 is the BMD insignia (shoulder patch), and I must admit that not everyone — not even in Huntsville — knows what BMD is. In the past you may have heard the Ballistic Missile Defense Program referred to as the ABM or Antiballistic Missile Program or Anti-Missile-Missile Program; or you may have

Ballistic Missile Defense Insignia

FIGURE 1

TABLE 1

PRESIDENT'S STRATEGIC WEAPONS IMPROVEMENT PLAN

- **IMPROVEMENTS IN COMMAND, CONTROL & COMMUNICATIONS**
- **MODERNIZE STRATEGIC BOMBERS**
- **NEW SUBMARINE LAUNCHED BALLISTIC MISSILES**
- **IMPROVE ICBMs AND REDUCE THEIR VULNERABILITY**
- **IMPROVE STRATEGIC DEFENSE (BMD, AIR, SPACE, AND CIVIL DEFENSES)**

heard it referred to by the name NIKE-ZEUS, NIKE-X, or SENTINEL or SAFEGUARD, or Site Defense, or Low Altitude Defense,and so on. Our job, simply put, is to develop for the United States an active defense against attacking intercontinental or submarine-launched ballistic missiles — active defense means that we somehow shoot them down.

We have been on a fast track since October because that is when Prsident Reagan announced his comprehensive strategic modernization program. The program — shown in Table 1 — has five mutually reinforcing elements. First, and perhaps most urgent, improvement of our strategic command, control, and communications systems. Second, modernization of the manned bomber force, first with the B-1B and later with the so-called "Stealth" bomber. Third, development of the new, more accurate and powerful TRIDENT II (D-5) submarine-launched ballistic missile. Fourth improvements in the accuracy and survivability of our land-based Intercontinental Ballistic Missile (ICBM) force. And fifth, improvements in our strategic defense including space defense, air defense, civil defense, and vigorous pursuit of our own BMD research and development.

BMD is also mentioned specifically in the element concerned with improving our land-based ICBM force, and this is the element which has probably received the greatest media attention.

Central to the Administration's Plan is development of the Air Force's new MX ICBM. The Carter Administration's proposal to develop 200 MX ICBM's among 4,600 horizontal shelters in the valleys of Utah and Nevada was scrapped. The Reagan Plan — shown in Table 2 — announced on 2 October 1981 was to deploy 100 MX with the first increment going into existing U.S. ICBM silos.

TABLE 2

ICBM MODERNIZATION PLAN

- **CANCEL CARTER MULTIPLE PROTECTIVE SHELTER PLAN**
- **DEVELOP & PRODUCE 100 M-X**
- **INITIALLY DEPLOY M-X IN EXISTING SILOS**
  - **— INCREASES US ICBM CAPABILITIES**
- **ACCELERATE R&D FOR 3 OPTIONS FOR PERMANENT BASING TO ENHANCE M-X SURVIVABILITY**

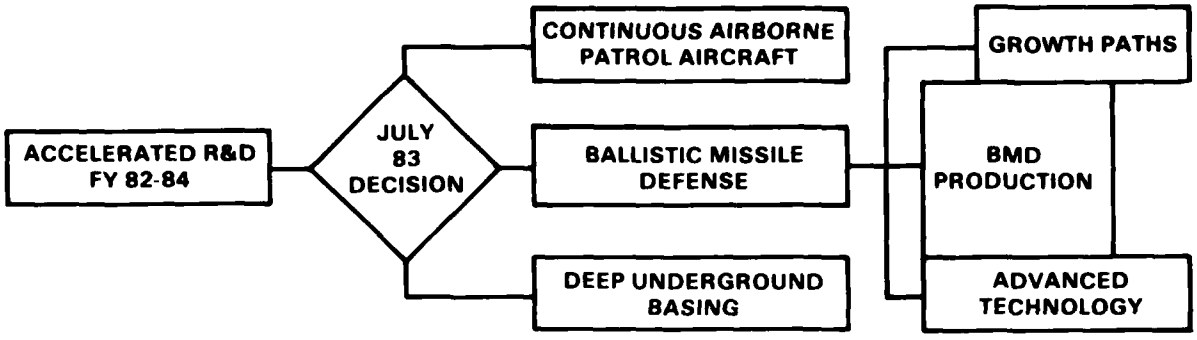


FIGURE 2

This was to give us improved ICBM capability. The MX is larger and more accurate than Minuteman; it would give us the hard-target-kill capability the Soviets already possess and which threatens the survivability of our ICBM's. Because the initial MX increment was not intended to be permanent basing for MX, the Reagan Plan included further research and development on three options for permanent MX basing which would increase its survivability.

The Administration's Plan calls for selecting one or more of the three options by July 1983 for development. As shown in Figure 2 BMD is one of the three options. The other two are the Continuous Airborne Patrol Aircraft, from which MX could be launched, and Deep Underground Basing, would place MX in a highly survivable environment and provide a fraction of the force with enduring survivability. Of course, if BMD is selected, it would mean a large production and development program. We would continue with the other efforts in our Systems Technology Program to develop growth paths that could be used in response to possible further growth and sophistication of the Soviet threat. We would also continue with our Advanced Technology Program, which is designated to identify and develop the kinds of technologies we will need for BMD growth beyond the current and maturing technologies

The effects of the Reagan Program on ballistic missile defense have been dramatic as shown in Table 3. Perhaps for the first time since the ABM treaty with the Soviet Union was signed in 1972, and certainly for the first time since the SAFEGUARD system was deactivated in 1976, the plan has reestablished ballistic missile defense as a serious strategic option for the United States. Another effect is that the Administration requested a total of $870.6 million for ballistic missile defense systems and advanced technologies for FY 83; that amount includes $727 million for systems technology, from which a deployment would come, and that is more than double this year's systems technology budget of $336 million.

TABLE 3

EFFECTS OF REAGAN PROGRAM ON BMD

- **REESTABLISHED BMD AS SERIOUS STRATEGIC OPTION**
- **MORE-THAN-DOUBLE BUDGET REQUESTED FOR BMD SYSTEMS TECHNOLOGY**
- **FOCUSED PROGRAM ON:**
  - **DEFENSE OF ICBMs BASED IN SILOS (DECEPTIVELY OR NONDECEPTIVELY)**
  - **SUPPORT OF POSSIBLE DEPLOYMENT DECISION BY JULY 1983**
  - **DEVELOPING MORE OF CAPABILITY INHERENT IN AVAILABLE TECHNOLOGY**
  - **DEVELOPING BMD GROWTH PATHS**

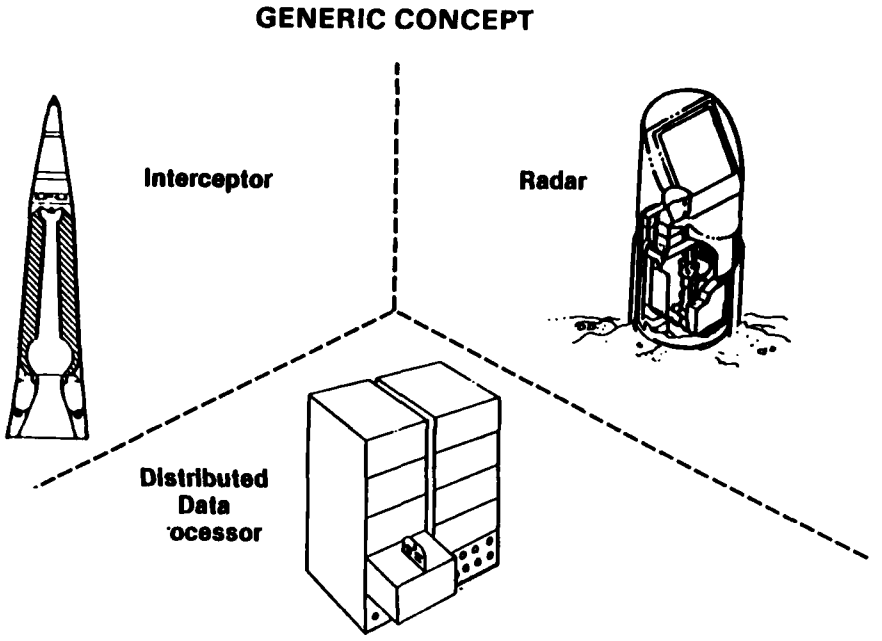


FIGURE 3

The Reagan Plan also refocused the BMD program: The principal thrust of the program is now specifically on developing a defense for ICBM's based, either deceptively or nondeceptively, in silos. Our near-term focus is on supporting a possible deployment decision during FY 83. Our focus also includes exploiting more of the capability inherent in the technology that we have been developing for low altitude terminal defense. For the future, the BMD program is focused on developing cost-effective growth paths for BMD if the Soviet threat continues to grow in numbers, quality, or both.

Figure 3 shows the generic concepts of the components that were being developed to defend the Carter concept of MX deployment. The components to defend the Reagan deployment of MX, whatever basing mode is finally chosen, will be quite similar. Because these components are very small, thanks to the revolution in miniaturizing electronic components, they can be based in a variety of ways. Consequently, whether the basing mode finally selected for MX is a fixed-silo mode or a deceptive basing mode of some sort, these components are being developed as a "common system" that will have sufficient flexibility to defend either basing mode.

The system I have been talking about as a candidate to defend the ICBM is what we call a "terminal" defense system. That simply means that it operates to intercept an attacking ballistic missile during the terminal portion of its flight, that is, after it has reentered the Earth's atmosphere and is streaking toward its target. Most of our work over the last 27 years has been in this regime; so understandably, these terminal defense technologies are the most mature and carry the least technical risk when it comes to developing a system from them. This is the background on BMD.

TABLE 4

BALLISTIC MISSILE DEFENSE (BMD DEPARTMENT OF THE ARMY PROGRAM REVIEW (DAPR)

- **DESCRIBED BMD PROGRAM AND INCREASED EMPHASIS**
- **DISCUSSED BROADER ARMY INVOLVEMENT IN BMD**
- **VCSA FOCUSED ON OPSEC**
  - **PROGRAM MAY MEAN OVERALL SURVIVAL OF UNITED STATES**
  - **SHOULD NOT COMPROMISE THROUGH POOR OPSEC**
  - **WHAT DO WE WANT SOVIETS TO KNOW**
  - **WHAT DO WE NOT WANT SOVIETS TO KNOW**
  - **ODCSOPS, OACSI, BMDO CONDUCT OPSEC STUDY**
  - **REQUIREMENT TO TIE OPSEC INTO OUTSIDE AGENCIES; I.E., AIR FORCE, OSD, ETC.**

Now let's look at OPSEC. During a BMD Department of the Army Program Review (DAPR), General Tate, our program manager was discussing the increased emphasis on BMD and the need for broader Army involvement in the BMD program effort. General Vessey, Vice Chief of Staff, Army (VCSA), expressed considerable concern about the technology loss to the Soviets. He asked about the BMD OPSEC program and focused on OPSEC, as listed in Table 4. He indicated that the strategic defense of the BMD Program may be the means of survival for the United States, and that we should not compromise the program through poor OPSEC. What BMD information do we want the Soviets to know? What BMD information do we not want them to know? He indicated that an OPSEC study should be conducted to assess the BMD OPSEC posture and to assess what information on BMD is in open sources. We should develop plans to tie BMD OPSEC into the U.S. Air Force, Office of the Secretary of Defense, Department of Energy, and the BMD contractors.

The Department of the Army (DA) Plan for BMD Operations Security — shown in Table 5 — places DA staff agencies and US Army commands under the samer "OPSEC" umbrella. The VCSA recently sent a letter to major commanders stating that "the BMD Program is of vital importance to the security of the United States. The Army is totally committed to improving OPSEC Army-wide and especially OPSEC as it relates to the BMD program. The importance of this program cannot be overemphasized, and I solicit your total support." The plan is to complement the Defense Investigative Service (DIS) program and emphasize protection of ballistic missile defense operations, tests, and experimental activities. The plan emphasizes for waivers when warranted by the OPSEC analysis process. The plan sets up procedures for coordination and establishes a vehicle for obtaining OPSEC support in other organizations involved in the BMD work.

TABLE 5

THE DA PLAN FOR BMD OPERATIONS SECURITY

- INTEGRATES ALL HQDA STAFF AGENCIES AND ARMY COMMANDS HAVING BMD RESPONSIBILITIES UNDER AN "OPSEC UMBRELLA"
- EMPHASIZES PROTECTION OF OPERATIONS, TESTS, ACTIVITIES
- EMPHASIZES PRACTICAL COUNTERMEASURES
- ESTABLISHES BASE FOR COORDINATION OF BMD OPSEC ACTIVITIES IN DOD, DOE, ETC.

TABLE 6

OPSEC PLAN CONCEPT

- BMDO, IN COORDINATION WITH ACSI, S & TIC, IDENTIFIES BMD INFORMATION THAT NEEDS PROTECTION
- BMDO IMPLEMENTS OPSEC INTERNALLY AND WITH ITS CONTRACTORS
- DCSOPS MANAGES OPSEC PROGRAM THROUGHOUT DA
- MAJOR COMMANDS AND AGENCIES DEVELOP OPSEC PLANS, TEST PLAN OPSEC ANNEXES, AND RISK ASSESSMENTS AND FORWARD TO DCSOPS
- DCSOPS APPROVES OPSEC PLANS, TEST PLAN OPSEC ANNEXES, AND RISK ASSESSMENTS
- INSCOM REVIEWS OPSEC EFFECTIVENESS AT EACH MILESTONE. INCLUDES OPEN SOURCE REVIEW, OPSEC PROBLEMS AND COST. PROVIDES FEEDBACK.
- DA OPSEC STEERING COMMITTEE IDENTIFY AND RESOLVE DOD, USAF, DOE OPSEC INTERFACE ISSUES

Our OPSEC planning guidance - shown in Table 6 - was that BMD would identify the BMD information requiring protection, implement OPSEC internally and with BMD contractors. Deputy Chief of Staff for Operations, Army (DCSOPS) would be the manager and require other commands and agencies to do OPSEC. In Table 6 the DCSOPS, as manager, would approve DA OPSEC plans and the U.S. Army Intelligence and Security Command (INSCOM) would monitor within DA and check for compliance with BMD contractors. The DCSOPS Steering Committee would obtain outside agency support. Now let's look at the OPSEC responsibilities for implementing the program.

The DCSOPS is the Army OPSEC manager; he appoints committees for coordination, and approves the OPSEC plans, as shown in Table 7. Assistant Chief of Staff for Intelligence, Army (ACSI) coordinates the scientific and technical review of BMD classification guides by the intelligence community. Also, ACSI coordinates intelligence support for BMD OPSEC plans - Table 7.

The INSCOM (902nd Military Intelligence Group) provides OPSEC support in developing plans and programs, conducts threat briefings, and checks for compliance with OPSEC plans, as in Table 7.

Major commands and agencies will designate an OPSEC manager who will be the point of contact for managing BMD OPSEC activities, as outlined in Table 7. They will prepare plans for protecting BMD operations and activities from Hostile intelligence collection. An OPSEC review will be conducted on information proposed for public release. They must include OPSEC in contracts when OPSEC is needed. Test plans must have OPSEC annexes outlining OPSEC measures to be taken during test efforts.

Major commands must assure that their contractors have the Industrial OPSEC Guide as well as classification guides - Table 7. OPSEC costs are to be documented and submitted at program reviews. Contracting officers should provide for the INSCOM advice and assistance in the BMD contract package.

The BMD Program Manager is responsible for preparing and furnishing the best available classification guides as in Table 7. He must assure that OPSEC is in support agreements. The BMD Program Manager receives all BMD information proposed for public release. He reviews all contracts to insure that contractors develop and implement OPSEC plans and identifies the cost of OPSEC.

I have talked a lot about OPSEC plans for BMD. Can you help with the OPSEC effort? Yes, by participating in the OPSEC program for your facility. Find out what needs to be protected in your organization's operations and activities. You, as a security professional, have a challenge. Talk with your project managers and find out how they are doing their work. Get involved with the operations. When was your last threat briefing? Do not be satisfied with marking and locking classified documents in a container if your operations and activities acan reveal classified information to advisary. Good OPSEC is necessary for a good security program.

COMMENTS ON OPSEC

Major General Winant Sidle, USA (Ret.)
Martin Marietta Corporation

I was invited to participate in this several months ago. We weren't quite sure at the time what the OPSEC situation would be; and consequently, as Elmer Hargis has just said, the Ballistic Missile Defense, Department of the Army (BMD DA) plan is being implemented, but from the standpoint of worldwide or Army-wide implementation is still underway. However, there is something that I would like to talk about. I'm going to play kind of a devil's advocate role here this morning becuse I think there are some points regarding OPSEC that everyone should think about. First let me say that I'm here as an individual rather than as a Martin Marietta representative, the reason being that we changed bosses this week and my boss hasn't seen what I'm going to say. So it's unapproved. No OPSEC involved though. Consequently, I will be talking.

TABLE 7

GENERAL BMD OPSEC RESPONSIBILITIES

- DEPUTY CHIEF OF STAFF FOR OPERATIONS (DCSOPS), HQDA:
  - SERVE AS THE DEPARTMENT OF THE ARMY OPSEC MANAGER FOR THE DEPARTMENT OF THE ARMY OPSEC PROGRAM FOR BMD
  - APPOINT A DEPARTMENT OF THE ARMY OPSEC STEERING COMMITTEE
  - COORDINATE AND OBTAIN DA APPROVAL OF OPSEC PLANS AND RISK ASSESSMENTS OF MAJOR ARMY COMMANDS AND AGENCIES INVOLVED IN BMD
- ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE (ACSI), HQDA:
  - COORDINATE THE REVIEW OF ALL BMD CLASSIFICATION GUIDES WITHIN THE US SCIENTIFIC AND TECHNICAL INTELLIGENCE COMMUNITY TO INSURE THEIR ADEQUACY IN DEFINING AND PROTECTING CRITICAL BMD SYSTEMS TECHNOLOGY, PRIOR TO PUBLICATION BY THE BMD PROGRAM MANAGER
  - COORDINATE INSCOM, AND OTHER NECESSARY INTELLIGENCE SUPPORT FOR THE BMD OPSEC PROGRAM PLAN
- COMMANDING GENERAL, INTELLIGENCE AND SECURITY COMMAND (INSCOM):
  - PROVIDE DIRECT OPSEC SUPPORT TO ALL COMMANDS, AGENCIES, AND CONTRACTORS PERFORMING BMD ACTIVITIES, TO INCLUDE NON-ARMY ELEMENTS
  - PROVIDE A DETAILED DESCRIPTION OF THE HOSTILE INTELLIGENCE THREAT (MULTIDISCIPLINE) DIRECTED AT EACH BMD SYSTEM, AT THE TIME OF BATTLEFIELD THREAT VALIDATION AND AT EACH DEVELOPMENTAL MILESTONE THEREAFTER
  - PROVIDE A REVIEW OF OPSEC PROGRAM EFFECTIVENESS AT EACH MILESTONE WHICH, AT A MINIMUM, INCLUDES AN OPEN SOURCE REVIEW OF BOTH GENERAL AND TECHNICAL INFORMATION CONCERNING BMD SYSTEMS UNDER DEVELOPMENT
- MAJOR ARMY COMMANDS, AGENCIES, AND ELEMENTS CONDUCTING BMD ACTIVITIES
  - APPOINT A BMD OPSEC MANAGER
  - PREPARE AN OPSEC PLAN FOR IMPLEMENTATION WITHIN RESPECTIVE AREAS OF RESPONSIBILITY TO PROTECT SENSITIVE BMD INFORMATION FROM HOSTILE INTELLIGENCE COLLECTION AND/OR EXPLOITATION
  - CONDUCT INTERNAL SENSITIVITY REVIEWS OF BMD INFORMATION PROPOSED FOR PUBLIC RELEASE

Continued

TABLE 7 — Continued

GENERAL BMD OPSEC RESPONSIBILITIES

- — SUBMIT ALL INFORMATION PROPOSED FOR PUBLIC RELEASE AT SYMPOSIA, CONFERENCES, BRIEFINGS, RELEASE TO MEDIA AND OTHER OPEN SOURCES TO BMDPM FOR REVIEW
- — CONDUCT SENSITIVITY REVIEWS OF ALL CONTRACTS PROPOSED IN SUPPORT OF BMD EFFORTS, AND REQUIRE CONTRACTORS TO DEVELOP AND IMPLEMENT OPSEC PLANS, IF APPROPRIATE
- — PREPARE OPSEC ANNEXES TO ALL BMD-RELATED TEST PLANS
- — DISSEMINATE CLASSIFICATION GUIDES TO ALL SUBORDINATE ELEMENTS AND CONTRACTORS PERFORMING BMD-RELATED ACTIVITIES
- — DOCUMENT INTERNAL COSTS, WHEN REASONABLY AVAILABLE, ASSOCIATED WITH OPSEC IMPLEMENTATION, AND PROVIDE SUCH DOCUMENTATION TO THE BMD PROGRAM MANAGER PRIOR TO EACH BMD SYSTEM MILESTONE/PROGRAM REVIEW
- — PREPARE AND SUBMIT OPSEC RISK ASSESSMENTS
- — INCLUDE A STATEMENT AUTHORIZING INSCOM ADVICE AND ASSISTANCE TO THE CONTRACTOR IN ALL BMD-RELATED CONTRACTS, IF THE SENSITIVITY REVIEW(S) WARRANTS INCLUSION OF OPSEC IN THE CONTRACT

- BMD PROGRAM MANAGER:
  - — PREPARE AND DISSEMINATE APPROPRIATE BMD CLASSIFICATION GUIDES TO ALL ARMY COMMANDS, AGENCIES, AND ELEMENTS, AND TO NON-ARMY ELEMENTS PERFORMING BMD SUPPORT FUNCTIONS, TO INCLUDE BMD CONTRACTORS
  - — CONDUCT PERIODIC REVIEWS OF ALL SUPPORT AGREEMENTS WITH NON-ARMY COMMANDS, AGENCIES, AND ACTIVITIES TO INSURE THAT SUCH AGREEMENTS PROVIDE FOR COMPLIANCE WITH THIS PLAN
  - — CONDUCT REVIEWS OF ALL INFORMATION PROPOSED FOR PUBLIC RELEASE AT SYMPOSIA, CONFERENCES, BRIEFINGS, AND OTHER OPEN SOURCES BY BOTH ARMY AND NON-ARMY ELEMENTS
  - — CONDUCT REVIEWS OF ALL CONTRACTUAL EFFORTS BASED UPON THEIR SENSITIVITY, TO INSURE THAT CONTRACTORS DEVELOP AND IMPLEMENT OPSEC PLANS
  - — IDENTIFY, WHEN REASONABLY AVAILABLE, COSTS ASSOCIATED WITH THE IMPLEMENTATION OF OPSEC REQUIREMENTS AT EACH MILESTONE AND SYSTEM/PROGRAM REVIEW

I'd better give you my credentials. I am responsible, among others — but I'm primarily responsible, for submitting material from Martin Marietta for security review clearance, for public release. That's one job. I have spent about 35 years in the Army, 20 of which were involved in security review from the other side of the fence, starting at DoD on down to post level. So I'm quite familiar with the security review process, and I think that's something we should talk about at this meeting because OPSEC eventually winds up in the security review area. And I think some points come out of this examination of it from a security review standpoint that need consideration.

In the first place, let me say that industry I'm sure is 100 percent in accord with the objective of OPSEC (I know Martin Marietta is). There's been an actual hemorrhage of material flowing out to the Soviets through open channels. Industry wants to cut that off just as much as anyone else. The question is, how do you go about it?

Industry does have then need for some publicity. You could say, one solution is don't say "nothing about nothing," and then you've solved your OPSEC problem pretty much. However, I don't think that will work. Take, for example, the value of favorable publicity to our country on certain of our weapon systems. Think about the M-1 tank. It's got a very poor public image. I've seen stories saying that its cost overrun is sixfold since 1972. Well, that's not true. The actual gain precentagewise in costs since 1972, in 1972 dollars, of the Abrams tank is only 19 percent. That seems a little high, but it's certainly not sixfold. This is where preplanned improvements that they were talking about in 1972 but hadn't worked into the project, such as the 120 millimeter gun turret. If you'd examine, in 1972 dollars, the actual cost overrun of the Abrams tank, it's only 5 percent. Now that's high, but it's certainly not sixfold. This is where someone has failed miserably in getting this word out to the public and to the Congress. There are many other examples of this type that I won't bore you with, but there are plenty of them. So I think from the standpoint of favorable publicity, it's necessary for the successful operation of our defense effort to be able to say something.

How about international sales? Mr. Reagan has asked us to try to sell things to our friends overseas. We can't do that without favorable publicity?

How about our engineers? Engineers are an unusual breed in that they love to publish. In fact, they have a saying — publish or perish. Well, there's high competition in industry for good engineers. If a firm says, "No, you can't publish," and another firm says, "Yes you can," you could get some engineers that way. So we have to take that into account at the industry level. I guess what I'm saying is we just can't shut off the flow of information to the public. So therefore, we've got a problem. We've got to figure out how to shut it off to some degree, to stop this hemorrhage.

Now as I said earlier, my particular area here is the security review of material proposed for public release and that includes technical papers, fact sheets, press releases, exhibit material, you name it — anything going to be shown to the general public. Now in industry the submission of this material for clearance is usually handled by public relations, which is why I'm here. In the Government, to me it's a little confusing these days because when you get below the top level there are different offices in some cases handling the security review process. At the Department of Defense, it's clear — The Office of the Assistant Secretary of Defense for Public Affairs is responsible for the final word, for saying that something is cleared for public release through his office of Freedom of Information and Security Review. At The Department of the Army, it's the same thing. It's a public relations area that does it —the chief of public affairs, which is another word for public relations. As you probably know, Congress won't let DoD use the word public relations. So they have to use public affairs. At DA there's an Office of Freedom of Information which works with the chief of public affairs who has the DA final say, in coordination of course with the OPSEC people.

Now I think I should say at this point that about three years ago under the instigation of the Department of the Army, Readiness Command (DARCOM) an OPSEC program was developed in the Department of the Army. It is not the same program that Elmer was talking about, but I'm sure it's closely related today. This program has been

implemented now for about three years, so I am able to talk about actual experiences with an OPSEC program. It will not be the final OPSEC program, I'm sure, but it is one.

As I was saying, I think there is some confusion in the area of responsibility in the field. I know for a fact that most of the installations we deal with, where we send material for security review, we send it through public affairs channels. However, in some cases we have to send it through contract channels; and in some cases we send it to the project manager or the program manager. Now all of these people have to see this material and pass on it I'm sure, and they do in most cases. But the point I'm trying to make here is that I think any future OPSEC plan should standardize how these things are handled in the field by the Government. In other words, one office should be responsible for coordinating the security review of a paper or whatever. And in my opinion since it's handled by public affairs at the top of the military, it should be that way in the field. I'm not saying cut out anyone else, but let the public affairs officer coordinate it. He has an advantageous position in some regards because he is fed material through the chain of command on sensitivities, on political aspects of various programs that don't necessarily get into the contracts area, that don't necessarily get into the program manager's area. he is also usually very well qualified to decide whether a paper or whatever should be cleared at the installation level or forwarded up the chain of command. We've had some experiences where that has been a problem.

Let me cite one example: We submitted a paper for clearance to an installation where the contract people were responsible for public affairs. (No offense please). In this particular case, it was run through the chain, was not run by the public affairs officer for some reason, and came back to us cleared. We published it and got an irate call from the Department of the Army. "Where did you get the authority to publish that?" Well, we had to tell them. It turned out that had it gone through the public affairs officer, it would have been bumped up the chain of command; and we would not have been able to publish the paper, but we didn't know that at the time. So I think the public affairs officer should be the coordinator of these things within the Government.

I'd like to get back to my main point about what have we learned from our experience with the Army OPSEC plan as it now stands and as it is now generally practiced in the field and our security review problem?

The security review process is time comsuming, as you know. The most efficient office we deal with in this matter is an Air Force office; and they guarantee us that if we get them a paper 30 days in advance, they'll give us an answer (yes, no, or amended) within 30 days. They require six weeks if the material is for use overseas or in the Washington, D.C. area, of if foreign nationals are going to be in the audience. I think that's interesting. They hold by this very well. So that's kind of an optimum *without* OPSEC clearance time.

Now what happens if you throw OPSEC into the pot? And I have to use the Army for this example because they're the only ones that are really practicing it at this time. We've had some pretty horrible examples. I'll just cite a couple.

One: We sent in our request for material to exhibit at a certain trade show — well ahead of the Army deadline given to use for submitting requests. The time approached. We shipped the material to the place where the trade show was going to be held. We kept calling and asking, "When are we going to get an answer? Is this go, stop, change?" The day that the show opened, I had to go to this spot because the Department of the Army said they would call me that morning with the final answer. They did, and they wanted to take out three different charts that were in the exhibit. As it turned out, we could do that by juggling things around and make the exhibit still look all right, but that is pretty close. I asked what happened, and the gentleman at the Department of the Army said, "Well, the OPSEC people got into this." Well, in this particular case, I'm not sure that's true. I think it was political more than OPSEC because it didn't look very classified to me. But anyway, that's what they said.

I'd like to read you another one. This is a case that we submitted to another installation. I just want to read you the brief answer I got back.

"Dear Sy, the attached package is approved for release except for the last

three pages. Even though information on those pages already has been published, and has been in the open for years, the security office feels that there is a need to try to protect the information still. This is the impact of the operations security (OPSEC) awareness that is currently circulating. It has command backing all the way to the Pentagon. I regret it took so long to reach this conclusion."

A third example: We submitted this particular case to still another installation in December of 1980. It was finally cleared with many amendments on the 18th of August, 1981 — that's eight months. When I looked at the changes, there were many notes, "for OPSEC reasons." But 12 of th 17 changes were deletions and some were even labeled "classified;; but didn't say what — just "Classified." In looking into the previous clearances of these items — these were all factual items — there were some philosophical items that I wouldn't argue with because that's a matter of opinion. If the Government doesn't want us to say something, we won't say it. But from the standpoint of facts, of these 12 , every one had been previously cleared more than one time. Several of the clearances went back six years, and in several cases the same facts had been cleared at least five different times. Now all of a sudden, they're classified.

This was addressed by Steve Garfinkel, and I agree with him. This is a very dangerous situation. You can't do that. I mean we all know that the Soviet intelligence collection program is excellent. If we put something out to the public six years ago, I'd say the chances of their knowing it are pretty good. We can be sorry about it, but we just have to forget it and not do it again. So as a result of all that I've been saying, I'd like to make a few recommendations to the people working on OPSEC. I think they should avoid *three* things, and I think they should do *three* things positively.

First, there's no point in trying to protect material that's already been released to the public. By released, I don't just mean cleared. I think it's important that this item actually be released. Some papers, or facts sheets or whatever, are sent in and are cleared; but maybe ther're not put out, so that's different. Bur once it's been cleared and released, it's gone — with the possible exception that Steve Garfinkel mentioned where it's only gone to one person and maybe he didn't do anything with it. But normally it's gone, so let's forget that.

The second point I didn't really talk about here, but it was discussed earlier is Freedom of Information (FOI) availability. If the material is available through FOI channels, we should either get it so it's not available or forget about protecting it. I don't think we should worry about that. I think we've got to solve that problem rather than try to spend money protecting it.

Cost — I haven't discussed that either because I'm trying to stay within the schedule here. I know a lot of you are aware of some of the studies that have been done about the costs if we had adopted the FOR OFFICIAL USE ONLY (FOUO) OPSEC solution or the RESTRICTED DATA OPSEC solution — it would have cost a bundle. And that money eventually comes out of the taxpayers' pocket, and I don't think that's a solution.

Now what is the solution? As far as I'm concerned, I think we should pay more attention to possibly actually classifying some of this SENSITIVE/UNCLASSIFIED information. The new Executive Order makes it clear that we don't have to identify the damage it would do to the country, but the classifier does have to do that or else he won't know whether or not it will do damage to the country. If it's SENSITIVE/UNCLASSIFIED, why is it sensitive? It is sensitive for intelligence reasons? Is it going to do damage to the country? I'd say if that's the case, let's classify it CONFIDENTIAL. Previous speakers have said that we can't really do that, but I think they're talking about red tape problems rather than reality problems. I think we could amend the rules to do this. I think it's a better system than trying to come up with some system that tries to protect additional information. Why don't we just classify it all to start with? I'm sure people will argue with me on that, but that's the way it looks from my worm's eye view.

Now getting back to my positive recommendations, I think one that the new plan should specify which field office in the military is responsible for security review. As I said earlier, I think it should be the public affairs officer; but whoever it is, it ought to be the same one every place.

If we can't classify all the material we're trying to protect, then I think we've got to have a simple system with clearly understood rules. Now I don't want to knock anyone in this room. I don't know who had a hand in preparing the document. But I think I read the original proposal out of OSD for an OPSEC temporary program at BMD, and it's hard to understand. We get so careful in our wording that the poor guy in the field has a great deal of trouble interpreting what the heck it says. So I think maybe it would be worth spending some money getting the thing written so that it's simple enough so a new guy coming in will know what's going on.

My final point — I think we should spend more time and maybe money in seeing if we can't classify more of this SENSITIVE/UNCLASSIFIED information. It seems to be that would really be a big step up in solving the OPSEC problem

Comment: We kind of think we invented OPSEC with the purple dragon out in the Pacific. We've just done an OPSEC plan with a major contractor, and we think it's working effectively from all the feedback. But if I could offer one comment endearingly, on OPSEC, security folks can't make it work. In all due respect, General, I also don't think public relations can make it work. We believe there is only one force in an organization that can make OPSEC work. It's not security; it's not public relations, and it's not the other array of support activities. Unless industry management is actually developing the OPSEC plan, we've never seen it work effectively.

General Sidle: Well, let me say, and I'm trying to speak for Elmer Hargis too, I think everyone agrees that that's true. And in our industry, at least in my company, and I'm sure in many others, the DIA office-type people are difinitely involved as Jim Buckland will tell you. But what you're saying, you've got to have command interest, and that is no doubt true.

Comment: I think one statement that General Sidle made, if we don't look at it very carefully and if we're not very cautious about it, it can be extremely dangerous, and that's the statement that "if it's releasable, don't worry about it; and don't try to protect it."

I know that the lock on my front door at home can be picked or slipped, but I still lock the front door. I don't hand the thief my valuables on a silver platter. The recognition in Government and in the Army is that although there are means, there are collection means that an adversary can use to get our information. And when we talk about unclassified information, the Freedom of Information Act is a means that can be used. We should still make him use his resources to get the information rather than providing it to him gratuitiously as we're doing now in so many cases. And one of the objectives of OPSEC is to make him expand at least some small resources to get the information rather than just handing it to him.

General Sidle: I perhaps didn't make myself clear. I was only talking about information that has already been released. For instance, I'll give you another example. Many years ago we had a fact sheet in the Department of the Army on the Lance Missile. This was handed out for 4 years. In about 1963 or 1964, somebody decided some of that material was classified; so the fact sheet, which had been released in actually thousands of copies, was declared CONFIDENTIAL. Now to me that is stupid. Although I wouldn't argue with your idea about making them work, I don't think there's a doubt in the world they haven't read and done any work on that one. And that's the kind of thing I'm talking about.

Mr. Hargis: I think Sy is primarily referring to a general rule that we agree to, but there are exceptions to that. Those exceptions, of course, involve situations where, over a period of time, the intelligence value the Russians have is diminished, and if you stop the flow of information, they lose confidence in their ability to use that information. If you cut off the flow over a period of time, you can gain some benefits from that.

Comment: I have difficulty believing that any really sensitive information hasn't been classified.

I guess I sort of agree with the General. If it's really sensitive, why the heck wasn't it classified to start with unless the classifiers simply weren't doing their job properly.

Mr. Hargis: The question was, why didn't we go ahead and classify the sensitive/unclassified information way back when? The problem was that you had to show identifiable damage under our old Executive Order. In some cases to show identifiable damage to national defense, or to some sensitive information of a targeting or intelligence nature, was most difficult to do. When it come in as FOI request, if it was in industry's hands and wasn't properly marked as classified or some other protective method, you had to release it. You couldn't then mark it and say, "Okay, now we're going to mark it." That was not authorized. So you ended up releasing very sensitive information.

Remember, we said that 90-plus percent of the information we're developing in a lot of technology areas is getting out within 6 months. That's a lot of information that we're handing to our adversaries. We have to stop that flow of technology. It started with the Freedom of Information Act. That was when we first started getting requests that we could not refuse.

Question: Does this mean, with the new Executive Order now you can go ahead and classify and get rid of this OPSEC stuff?

Mr. Hargis: No, it does not mean that.

Comment: You said you couldn't classify it because you had to prove identifiable damage. The term identifiable is now gone.

Mr. Hargis: His question was, Now that you can classify it, can you do away with OPSEC? The answer to that is no, because there's still operations and activities and tests that are not covered under the industrial security program that have to be protected to protect the technology. And each organization has to look at those things that they do under contract, if it's a contractor, to determine how they can best protect that information that requires protection.

Question: We're talking about information that is not covered under the industrial security program in this OPSEC business. Then why is it showing up in 254s?

Mr. Hargis: That's a good question and I think it deserves an answer. He said, why is it in 254s? We've had some growing pains in implementing OPSEC in BMD. We initially started out including it in a DD 254 because it seemed to be a vehicle to get some action going. And remember, we've got a deployment decision facing us in mid-1983. So as a result, we had to get something out on the street to protect the BMD technology. We started only referencing in a DD 254 the requirement for OPSEC, and it is a contract provision, special contract provision within the BMD contracts, requiring that the contractor do OPSEC if he's involved in operations, activities, and testing that requires OPSEC.

Comment: I believe the BMD has two security classification guides — one on systems technology and another on advanced technology. I believe that those guides could be revised under the forthcoming Executive Order to cover a good portion of information that has been previously expended to the public in one means or another. And information developed after or on the 1st of August could become classified to cut a lot of work on the part of many people under the OPSEC program, because if the information is classified, it does have a definite protection which everyone understands. But trying to protect unclassified information is very hard because it is not identifiable.

Mr. Hargis: What he's saying is we need to redo our classification guides on the BMD and include in those some of the things that we've been losing in the technology area. We agree with that. We are currently revising our guides. The project people are going over them. We've provided some of them to industry for their review. As those come back in, we hope we'll get the guide out sometime in August. We think it will be in the hands of the people that need it before that date. But we agree that that's the way to solve part of the problem

But there again, we in BMD do not know in all cases how you, as a contractor, or you, as government personnel, are going to do your job based on the support agreement or tests in the contract. So you have to evaluate that and determine how you're going to do that job. The security people and

the operators have to get together, and I don't believe that the operators alone can do it. I don't believe the security people alone can do it. I think it has to be a concerted effort and a lot of work, between the operators or the contract managers or the people that are in charge of the project and the security department, to get a proper product out.

DEFENSE INVESTIGATIVE SERVICE PROGRAM UPDATE

Thomas J. O'Brien
Director, Defense Investigative Service

As always, it is a distinct pleasure for me to be with you today and share in your deliberations about the security of our Nation and particularly industrial security. Among you are many old and valued friends with whom I have had the pleasure of many years association. For me, this year is a bit different from the past. This is the first time I have appeared before you as the Director of the Defense Investigative Service (DIS). This is my first opportunity to tell you "The DIS Story" — the 1982 version.

DIS Mission

DIS was established in April 1972. It is a separate DoD agency under the direction of the Deputy Under Secretary of Defense for Policy. DIS has a budget of $98,000,000 with 3,470 assigned personnel. DIS is charged with two basic missions: investigations (personnel security investigations and leaks) and industrial security (three programs — defense industrial security; defense industrial facilities protection; and arms, ammunition and explosives programs).

I would like to discuss our investigative mission with you at the outset since personnel security investigatiions are the basis for security clearances. We are charged with the fulfilling of the personnel security investigative requirements for all DoD military and civilian personnel as well as contractor personnel working under the auspices of the Defense Industiral Security Program. With respect to contractor personnel, there has been a marked increase of contractor clearances in the past several years. Contractor investigations were about 10 percent of our investigative workload for a long time, and now they are up to 25 percent. This increase reflects our national commitment to defense. It also reflects a significant workload increase for us as well as an increase in your concern that we accomplish our tasks in a timely mannner.

Personnel Security Investigations (PSI) Workload

During the last 12 months, we have significantly reduced the number of pending PSI cases. As of 30 April 1982, this figure has been reduced to 65,565. In February 1982, DIS had a record closing figure of 77 more cases closed per day than opened. In March we closed 110 more cases per day than opened; and in April, 221 more per day. Our current goal is to reduce the backlog to manageable level of under 52,000 cases by the end of this fiscal year. To accomplish this goal we have increased our corps of special agents and developed many management improvements.

PSI Resources

The number of personnel authorized DIS-wide for the investigations mission and the number of investigations — Background investigations (BI) and Special Background Investigation (SBI) are as follows: At DIS inception in 1972, we had an authtorized manpower level of 3,000; the number of pending requests at that time was 41,304. In 1976 DIS experienced a drastic cut in personnel and by 1980 we were down to 1,740 authorized postions. It is significant to note that when we were at our lowest manpower level, we were also at our highest level of backlog — 84,250 cases pending. However, now we have been authorized additional personnel; and as our resources have gone up, our pending caseload has gone down. As of April 16, 1982, our backlog was reduced to 66,109.

Turnaround Time

As we work on reducing our pending case backlog, we are also working to reduce the turnaround time on BIs and SBIs. Our current turnaround time for these types of investigations is about 174 days; our goal is to reduce that number to 65 days. As our resources continue to be augmented, and bar-

ring any unforeseen circumstances, we are confident we can meet this goal.

So far i have told you about our personnel security investigative mission and our efforts to produce results sooner. Now let's look at the personnel security investigation (PSI).

Investigations

A PSI is an investigation to determine an individual's eligibility for access to classified information, assignment or retention in sensitive duties. These investigations are designed to develop information pertaining to an individual's loyalty, character, emotional stability,trustworthiness, and reliability by conducting appropriate record checks and interviews. Our investigations frequently deal with such serious issues as subversive affiliations, use of illegal drugs, excessive use of alcohol, hostage situations, and excessive indebtness. Additionally, DIS conducts post-adjudicative investigations on individuals who have already been granted access, when allegations are made reflecting unfavorably upon that person's character.

Investigations are "Big Business" in the DoD. DIS currently conducts PSIs for over 2,700 requesters. Annually, we do approximately 185,000 field PSIs. We also conduct National Agency Checks (NACs) for all of DoD. Including entrance NACs, and the total number of NACs we process yearly is now approaching the one million mark. When you consider the size of the Department of Defense, the 400,000 new recruits each year, and the number of DoD contract facilities, the reason for these high numbers is readily apparent.

Recently, we have made significant management improvement in the conduct of background investigations. In fact, I believe it is a major breakthrough in the entire concept of PSIs. it is known as the Interview-oriented Background Investigation (IBI). Since the days of World War II, background investigations have been done in the time-honored manner of interviewing former employers, associates, neighbors, teachers, and others to obtain the necessary information about an individual. These contacts, plus the NACs, constitued the scope of the background investigation. This *Modus Operandi* served us well for decades. However, in recent years security has changed. Neighbors no longer know who lives next door, former employers are hesitant about releasing information as well as criminal justice actitivites because of privacy act constraints. In short, it is no longer possible for Federal Investigators to obtain a true picture of the subjects of investigation.

Our new approach is based on the concept of going to the best source first-the individual himself/herself. In-depth comprehensive interviews with the subject have proven most successful. People like to talk about themselves — that's a psychological fact — and they will disclose the varied facets of their lives, many of which are derogatory as well as complimentary. Of course, we pursue the information that the subject tells to verify the facts and round out the investigation with a true and complete picture of the individual. Further, the NAC is conducted in all cases. Our analysis of IBI results versus the traditional BI method has sustained our belief in this new approach. In summary, we beleive the IBI is a quality investigation for the following reasons:

1. The subject has the greatest range of information.
2. The subject has the greatest detail and mitigating facts.
3. The subject interview avoids problems of references "drying up" under Privacy Act and the PSIs.
4. It focuses on issues very quickly, avoids the "shotgun approach" and saves a great deal of investigative time.

(Thus, the quality continues even as we expedite quantitative productivity)

In addition to PSIs, DIS also conducts other investigations as directed by the Office of the Secretary of Defense. We are currently tasked with the responsibility to investigate unauthorized disclosure of classified information matters. The protection of classified defense material is a responsibility that most individuals accept and fulfill. However, on occasion, an individual will deliberately or inadvertently disclose classified information to unauthorized recipients. Their motives for acting this way are varied: Where some feel strongly about the political or economic aspects

about defense programs, others may simply see such an act as a way of obtaining the interest and company of some individual. When information is disclosed, the DIS just then conduct an investigation to identify the source of the data and the motive for the disclosure. In this way, the appropriate adjudicating agency or person can ensure that the proper corrective action takes place. This is a time-consuming type of investigation which is managed out of the DIS headquarrters to ensure expeditious handling and continuity of effort on the part of investigators.

Our companion mission is the administration of DoD Industrial Security Programs. We are responsbile for these separate programs that, while not co-equal in size, are co-equal in our management concern for their effectiveness and success.

Industrial Security Programs

The Defense Industrial Security Program provides for the safeguarding of classified information entrusted to industry in connection with defense contractors. In addition, the program provides security administration for 17 other departments and agencies in the executive branch of Government. Approximately 11,400 cleared facilities that employ some 1.4 million cleared personnel are under the Defense Industrial Securfty Program.

The Defense Industrial Facilities Protection Program involves some 2,200 facilities which have been identified as critical in times of national mobilization. DIS periodically surveys these facilities to assist management in maintaining a good physical security posture and to assist in the development of contingency planning programs.

The DoD Sensitive Conventional Arms, Ammuntion and Explosive Program involves the inspection of approximately 300 contractors who have custody of sensitive conventional arms, ammunition or explosives in connection with DoD contracts.

In our role as administrators of these Industrial Security Programs, we implement the policies promulgated by the Deputy Under Secretary of Defense for Policy. We monitor contractor compliance to DoD requirements and recommend to DoD, policy adjustments to ensure that requirements and procedures stay in tune with real-world situations and abreast of changing times.

Now, I would like to discuss several specific areas of concern with respect to the Industrial Security Programs.

Unannounced Inspections

We are now conducting unannounced inspections as a regular part of our Defense Industrial Security Program. We are requiring that at least 5-percent of our annual inspection effort be unannounced and apply across-the-board to all types of facilities.

Let us look at some of the results of our unannounced inspection efforts. In February 1982, we conducted a total of 1,189 inspections of which 77 or 6.19 percent were unannounced. A comparison of the results shows that 39 percent of the announced inspections resulted in minor deficiences requiring a letter of requirements to facilities, while 52 percent of the unannounced inspections resulted in minor deficiencies. One percent of the announced inspections resulted in Major deficiencies while 4 percent of the unannounced inspections resulted in major deficiencies. There were no unsatisfactory ratings.

More deficiencies were found in the unannounced inspections than in announced inspections. While we are not sure of the difference in results (and we are studying the matter) we can say with certainty that overall inspection results show that the vast majority of facilities have fine security postures; they are doing their part in our common effort — the protection of classified information.

Foreign Ownership, Control or Influence

At this juncture, I would like to bring you up to date regarding the events we are currently experiencing with respect to our foreign ownership, control or influence, or what we call "FOCI" policy.

In Congressional testimony last November, I described the underlying basis for our FOCI policy as follows:

"If the top management of the company

consists of a foreign entity or is under the influence or control of a foreign entity, it would not be reasonable to entrust them with classified information which is not releasable to the foreign principal or owner. As a minimum, it would establish an untenable conflict of interest. As a maximum, it would be entrusting classified information with those whom national policy has dictated should not have it — for example, the foreign government itself."

This philosophical basis is so reasonable that it has never been seriously questioned. Nevertheless, over the years we have been presented with innumerable proposals for a more liberal application of these principles. In all of those cases, we were able to clearly demonstrate that the national security interest would not be served by any relaxation of the manner in which we apply the Department of Defense FOCI policy. With this as background, you'll be interested to know that the current Congressional interest *is not* in the direction of relaxing the policy

The November Congressional Hearing concerned a foreign acquisition of a U.S. firm which was not in the Defense Industrial Security Program. I was asked to testify for the purpose of explaining the DoD FOCI policy and outlining the measures that the DIS would have taken if that firm were under our purview. The record of those hearings will show that the Committee thought that our methodology for dealing with FOCI in cleared contractor facilities is commendable. The Committee also expressed concern that it is only the Defense Industrial Security Program which has a comprehensive system for ferreting out FOCI. Moreover, the Committee was concerned that foreign acquisitions of uncleared firms could lead to the transfer of cumulative technical expertise to a foreign government.

Congressional interest did not end there. Beginning in February 1982 and concluding with open hearings on April 6, a subcommittee of the House Government Operations Committee thoroughly reviewed the manner in which DIS handled a FOCI case regarding a firm which had only 5.9 percent of foreign ownership and about 29 percent of foreign-source income. I am glad to report that our decision to allow that contractor's facility clearance to remain in effect was found to be clearly in accordance with the DoD FOCI policy. However, the chairman of the subcommittee suggested that the overall policy for handling of these cases should be tightened even further.

The message from the Congress is clear. First, foreign investment in U.S. industry remains a matter of priority concern. Second, when cleared contractors are involved, our handling of these cases will be subjected to close scrutiny. In light of these developments, I would like to remind you of the FOCI reporting requirements contained in paragraph 6a(4)(f) of the Industrial Security Manual. Discussions or negotiations which may be expected to lead to an increase in your firm's foreign involvements must be reported to the Cognizant Security Office. When you do this, your Cognizant Security Office will be able to advise you of the impact that the proposed new FOCI elements may have on the facility security clearance. In such cases we are often able to suggest modifications or alternatives that we can accept under the policy without a disastrous effect on the facility clearance. On the other hand, when we are presented with a *Fait Accompli* we must apply the policy to the new facts as they then exist. Quite often, we have no alternative but to invalidate the facility security clearance. With advance notification and a team approach we can work together to minimize any adverse impact on existing facility security clearances.

Last October we enacted a much more restrictive policy concerning the clearance of immigrant aliens having access to classification information in the industrial environment. This tighter policy was not conceived precipitously. Only after a great deal of study and actual experience gained from the government environment was this policy imposed on industry. I might also add that this restrictive approach is in keeping with the procedures of other countries with whom we have security agreements.

Since implementation of the change regarding personnel security clearance for immigrant aliens, The Defense Industrial Security Clearance Office (DISCO) has processed only three such cases. These possessed special expertise that would have been lost to the Government and their employers, had these clearances not been processed.

Certain restrictions have always been applied to clearance granted to immigrant aliens. These restrictions continue to remain in effect and apply to those few critical immigrant alien clearances granted since implementation of the current policy. So that there will be no misunderstanding the effect of these restrictions, I want to emphasize at this point that, should an immigrant alien occupy a principal officer position — one that requires that he or she be cleared as a part of the facility clearance — these restrictions will apply to the entire facility and all personnel clearances granted to that facility despite the fact that all other personnel are U.S. Citizens. Carrying this step further, these restrictions will also apply to any subsidiary of such a facility.

In the near future, the employers of immigrant aliens who were cleared, or in the process for clearance prior to October 1981, wiill be queried by DISCO concerning the current status of such employees. Employers of cleared immigrant aliens will recieve a letter from DISCO that will request information concerning the current employment status of the immigrant alien. In addition, the employee will be requested to verify the current citizenship status. If the subject is still an immigrant alien, verification of the permanent residence date will be required. The employer will further be requested to determine whether or not the immigrant alien has applied for U.S. Citizenship. If there has been no action taken by eligible immigrant aliens to obtain citizenship and no extenuating circumstances exist, action may be initiated to administratively terminate the personnel security clearance.

DD Forms 48 and 49

For some time, we have been attempting to revise the Industrial Personnel Security Questionnarie — DD Forms 48 and 49. This effort has had the assistance and advice of some of you. We are making progress in this effort, although not as quickly as I had hoped.

After a number of iterations, the final approved versions of the new DD Forms 48 and 49 were returned to the Deputy Under Secretary of Defense for Policy (DUSD(P)) from the Defense Printing Office in the form of camera-ready masters. As of March 31, 1982, copies of these masters were forwarded to the Office of Management and Budget (OMB) for their approval. Past experience indicates that we can expect this approval to require up to 90 days. While we would like to say that the forms will be available from DISCO in 6 to 8 months, information from DUSD(P) indicates that we should not be too optimistic. Our recent experience has shown that it is becoming increasingly difficult to accomplish the necessary PSIs requisite to a personnel security clearance without an authorization to release information from the subjects of those investigations. Therefore, in the Industrial Security Letter (ISL) which was recently distributed, we are establishing a requirement, pending a formal change to the Industrial Security Manual, that a DoD Authority Release of Information and Records Form (DD 2221) will be completed and atttached to each submission of a Personnel Security Questionnaire (DD Form 49). This release form will authorize our investigators to seek information from schools, landlords, employers, criminal justice authorities, etc., to more expeditiously accomplish the investigations and ultimately grant security clearances to you in shorter periods of time. The release from will be stocked at DISCO as quickly as possible and will be furnished to the contractors automatically when they are supplied with DD Forms 49. Cognizant Security Offices will also be provided a stock of these forms to assist you in the processing of Officers, Owners, Directors, and Executive Personnel (OODEP) clearances or in other instances where you may need them. The revised forms, which are presently in the process of being approved by OMB, and which we hope will be available for you later this year, will have a release form as an integral part of the package.

The New Executive Order 12356

On April 2, 1982, Executive Order 12356, concerning "National Security Information" was signed by the President. This EO supersedes EO 12065 and becomes effective August 1, 1982.

The development of the new EO began in early 1981 within the executive branch in order to update classification regulations on the basis of current experiences. The Order was formulated following consultation with Congressional Com-

mittees and representatives of non-government organizations.

The basic objective of our National Security Program is to ensure that the public domain is informed about our Government's activity and that sensitive information relating to our national defense and foreign policy is protected. The order will facilitate the public's access to information about the affairs of Government when disclosure will not damage national security. At the same time it will permit the Government to classify that information when unathorized disclosure could cause damage to the national security.

It will be necessary to amend the Industrial Security Manual (ISM) to reflect the policy announced in the new EO. However, pending publications of revisions to the ISM, the current provisions will remain in effect. Information concerning changes to the ISM will be published in the near future.

In accordance with ISM provisions, contractors should continue to review their classified holdings for disposal of unneeded material. This action will serve to reduce the risk of compromise and lessen the administrative costs associated with safeguarding the classified material involved.

Let me highlight some steps being taken at the Defense Industrial Security Institute (DISI) in Richmond, Virginia

Counter-Awareness Briefing

DISI is now augmenting its traditional classroom training in security with a Security Awareness Bulletin. The bulletin is sent to each facility in the Defense Industrial Security Program. To date, there have been three issues. The fourth issue is scheduled for May 1982. The primary purpose of the bulletin is the hostile intelligence threat to U.S. industry. We hope the bulletin has been of assistance to you in meeting your requirement to give cleared employees indoctrination in the method and operation used by hostile intelligence services.

The May issue will include an expanded bibliography of audiovisual materials currently available to contractors through the DoD audiovisual distribution system, as well as materials through other means. Instructions on how to order these materials will be included.

We are reviewing the programs of instruction for all our courses to assure that they are up to date and reflect current policy direction as given to us by DoD. In addition to the course traditionally offered to Government and industry, the Institute is now the center for the training of our investigators in the techniques of investigations, — specifically, or how to accomplish PSIs.

Earlier I discussed our investigative workload and the fact that industrial requests equate to about 25 percent of that work. How does this translate to DISCO who issues the clearances?

DISCO Clearance Goals

Actual increases of clearance requests have been averaging 5½ percent a year. By comparison in FY 1979 workload was 145,000; 1980 was 156,000; 1981 was 161,000 and projected workload for FY 1982 is 170,000. By March 31, 1982, 85,000 clearances had been issued by DISCO — 1,000 above the projections for this period.

DISCO Workload

The average time to finalize TOP SECRET clearance requests was 185.30 days in January 1982, and this has been reduced to 149.5 days in June 1982. The total grant elapsed time (calendar days) is from the date the clearance application is received to the date the letter of consent is issued. Average time for SECRET clearances peaked at 121 days in June 1981 but has now been reduced to 80.6 days; this includes time of DISCO as well as non-DISCO time.

Non-DISCO time is a composite of the following time:

1. Resolving contractor rejects.
2. Accomplishment of the investigation by the DIS.
3. Additional information requested from the contractor.
4. Case is at the Defense Industrial Security

Administrative Review (DISAR) board.

5. Any other time that DISCO does not have direct control of the request for clearance.

DISCO time was 8.2 days in June 1981 and is 7.3 days as of June 1982. DISCO time is time required by DISCO to accomplish administrative processing of the clearance application. This includes:

1. Screening of the Personnel Security Questionnaire.

2. Request to the Personnel Investigative Center (PIC) for investigation.

3. Making a security determination.

4. Issuing a letter of consent.

To accomplish our dual missions, we are constantly striving to effect management inprovements that will improve efficiency and economy. During the past year, a team from the program standards division, Directorate for Industrial Security, has visited each Cognizant Security Office and most field offices. The purpose of these visits was to determine if all offices were operating in a like manner and that uniform requirements were being imposed nationwide. This is particularly important for multi-state companies. Based on our findings from these visits, we have issued operating instructions that were designed to assure standardization. We hope there are fewer variances because of our efforts.

On February 14, 1982, the New York Cognizant Security Office was merged with the Philadelphia Cognizant Office. As a result of this merger, all facilities in the state of Virginia that were under the cognizance of Philadelphia, are now under the cognizance of the Washington, D.C. Cognizant Office.

On July 1, 1982, the Kansas City DIS Region will be merged with the San Antonio DIS Region. St. Louis will be the Region Cognizant Office with the Dallas Cognizant Office being merged with St. Louis. The current Kansas City Region (St. Louis Cognizant Office) will be divided between the San Antonio Region (St. Louis Cognizant Office) and the Chicago Region (Cleveland Cognizant Office).

Government/Industry Partnership

In closing, I want to bring up a theme that most of you have heard me expound on many times —the Government/Industry partnership that is the cornerstone of the administration of the Defense Industrial Security Program. The Security Manager is at the facility day-in and day-out; we aren't. We monitor your program periodically in order to provide advice and assistance, but it is the Security Manager who administers the program. It is only through our working together in this manner that we can continue to maintain an effective security program. I pledge to you our best efforts to accomplish our investigative tasks with dispatch and our continuing active role as your partner in the full gamut of industrial security.

DIS UPDATE OF ACTIVITIES, REQUIREMENTS AND AREAS OF EMPHASIS (DIS PANEL PRESENTATION)

Thomas J. O'Brien (Moderator)
Director, Defense Investigative Service

Richard F. Williams
Chief, Industrial Security Program Division, DIS

Joan Turner
Director, Industrial Security
New Orleans Region Director

Sandy Waller
Senior Staff Specialist
DIS Headquarters, Washington, DC

Thomas J. O'Brien: I am very pleased and priviledged to have this opportunity to share the podium with three of my very distinguished colleagues from the Defense Investigative Service (DIS). They're going to have short presentations, and then we are open to questions and discussion. We hope to be able to clear up a little bit of the chaos in the industrial security program. I'm going to introduce our three speakers all at once. Our first speaker this morning will be Mr. Richard F.

Williams who is Chief of the Industrial Security Program Division in our headquarters in the DIS. He is going to speak on the organizational aspects of the industrial security program. Following will be Mrs. Joan Turner. Her headquarters are in Atlanta, and she is responsible for the industrial security administration of all of the southeastern part of the United States, roughly that area south of Richmond and east of Texas. Then will follow Ms. Sandy Waller who is the first person to hold a postion that has exclusive responsibility in the headquarters policy staff for classification management matters. She's going to talk about some changes to the Industrial Security Manual (ISM), particularly those necessary because of the new Executive Order 12356.

Richard F. Williams: I'd like to briefly go through our organizational structure. Many of you have asked questions about the DIS organization — how we administer the industrial security program. The DIS was established in October of 1972. It was a compilation of resources that came from the military departments. Starting in October of 1980, there were three programs transferred to DIS. Speaking personally, I was very pleased to see this. I was so discouraged before that so I left and went to the Navy. I enjoyed my tour there, but I came back to the DIS after it was transferred. It was a very discouraging thing to see the resources base deteriorate 35 to 40 percent after putting a lot of time and effort into the program, such as the industrial security program. I'm happy and pleased to see that trend reversed now.

We have three programs: the defense industrial security program, the defense industrial facilities protection program, and the program for safeguarding conventional arms, ammunition, and explosives. The defense industrial security program is the one that I'm primarily involved with as the Chief of the Industrial Security Program Division. Most of you are involved with that program.

Mr. Joseph Grau has commented that President Eisenhower was involved in many of the training films. Executive Order 10865 was signed by President Eisenhower, so most of the films that you see that start with the industrial security program are going to mention that particular Executive Order.

I'd like to tell you a little bit about the scope of the industrial security program. First of all, we have about 17 non-DoD user agencies. GAO just recently signed an agreement, so that will be the eighteenth. I believe the last industrial security letter in 1981 mentioned that the Federal Reserve Board had been added. Those are the new ones that we've added. We have approximately 11,500 contractors, and that varies on a day-to-day basis, and about 1.4 million cleared personnel, and about 12 million classified docuents. Approximately 95 percent of those documents are in less than 5 percent of the large facilities. Those facilities usually have professional security staffs. The smaller facilities primarily are where the violations seem to occur. We have about 4,500 approved automatic data processing systems that will be a subject of discussion later.

We implement the government Industrial Security Program with the Industrial Security Regulation (ISR). We recently had the same problem Mr. Arthur Van Cook had, and that was to completely revise the numbering system of the ISR. I'm pleased to see that Mr. Van Cook and Mr. Thomas O'Brien, have provided us with an exception to that policy, so we'll be able to continue using the old numbering system. This is very important because we might have found ourselves in a position of having to change contract documents of all types, instructional aids, and many things on the user agency side.

In industry we implement the industrial security program through the Industrial Security Manual (ISM), the Communication Security (COMSEC) supplement to the ISM, and also the Garrier supplement. Let me mention briefly the changes to the ISM. We have some pending chnges, and we're trying to get together a change package that will incorporate some approved changes. Regarding the COMSEC supplement to the ISM, we have been loboring with that for about seven years. We hope to get that out for recoordination. It should be out by the time I get back to the office.

In relationship to the COMSEC supplement, we're very pleased with the help and assistance we've received from both industry and from Government on the part of The National Security Agency. We had working groups that were put together as industry groups. And we found ourselves in the-

middle between a 180 degree difference in position. So we tried to reconcile those positions, and we hope the product that's coming our for recoordination does reconcile those two positions.

We implement the industrial security program in industry by an agreement with industry. All of you are familiar with that. That's the 441 agreement, and it's complemented by the 441-S which is the document that relates to foreign ownership, control, and influence. I'll just give you a quick glance at different things we do on a facility clearance. Basically, we go out and do the survey. We help the contractor develop a standard practice procedure. We don't say, "Here it is. Implement it." We try to assist you. We have a four fold job that will be mentioned by Mrs. Joan Turner, and helping you is a part of that job. Compliance is also a part of that job, but I think if we help you properly then perhaps we don't have to deal so much in the compliance arena.

Briefly I would like to go through the organization. Up at the top of the scale is General Richard Stilwell. Above him is the Secretary of Defense, Mr. Casper W. Weinberger, and his Deputy is Mr. Frank Carlucci, III. Then the Under Secretary of Defense is Mr. Ikle. Directly under him is General Stilwell.

General Stilwell has two individuals that are under his conizance that feed directly into the industrial security program. They are Mr. Maynard Anderson's group and Mr. Art Van Cook's group. You'll see this later when we talk about ADP policy.

Mr. Thomas O'Brien falls directly under General Stilwell. Under Mr. O'Brien are the DIS Regional Directors. It's a line relationship. Under the DIS Regional Director is the Director of Industrial Security, and the field offices fall under the Director of Industrial Security.

My immediate boss is Mr. Frank Larson and his Assistant Deputy Director for Industrial Security is Mr. Ray Nels. They have program management responsibility over the Industrial Security Program. They give guidance and instructions down to the region level, but it's not a direct line relationship. As a program manager, they make many inputs regarding resourcing, funding, and all aspects of program management.

We have a brief breakdown of the field structure in the region. There's a Director for Investigations on the same level as the Director for Industrial Security.

We have in the headquarters element the Facilities Division and the Operations Division. The field offices fall directly under the Operations Division. Many people consider the Facilities Division staff. I'd like to disspell that immediately. They are not staff. They perform many critical functions, and they perform a straight working-type of relationship because they have an assignment that involves them to perform the work. They don't just simply vie to the director of industrial security. That's not the way it works in the regions, and I wish to emphasize that.

Under the Director of DIS we have Mr. Frank Larson. Then we have the three main field extensions. Those are, Defense Industrial Security Clearance Office, (DISCO) Defense Industrial Security Institute (DISI), and Overseas Security Investigation (OSI). Most of you are familiar with those three different organizations.

There are three divisions that fall directly under Mr. Frank Larson at headquarters. I'm the chief of the Industrial Security Division. We have a chief of the Industrial Facilities Protection Division, and we have a Industrial Security Standards Division. Basically the breakdown is that anything to do with industrial security as far as a policy relationship would come over to my shop. If it's the industrial facilities protection program or the arms, ammunition, and explosives program, it would go over to Mr. Donald Richardson's shop. If it's standards as far as checking our operational standards, it would belong to Mr. John Hancock.

It was mentioned by Mr. Joseph Cooper that sometimes you have questions about the industrial security program. If you have questions, generally it's going to come up to my shop. We're broken down into work groups. We have a group that handles ADP security, one that handles international, one that handles clearances and one that handles foreign ownership, control, and influence.

I'd like to mention just a few areas where we can work together on the user agency side. First, a change has occurred, and I'm sad to report this. In the user agencies, they used to make helpful

recommendations on a regular basis. Now they are sporadic. I would like to see that renewed. I would like to see the user agencies make positive recommendations to use. If you see something wrong with the ISR ot the ISM, let us know. We'll try to do something about it. As you know, we don't approve the policy. Our boss, General Stilwell, does that. We can make the recommendations and the proposals, and we certainly are willing to do that.

User agencies have to give sound classification guidance to the contractors. It is very difficult to go to that contractor with poor guidance and expect him to do a proper job. I believe that's the keystone of the Industrial Security Program. There are two things — Education and Training and Classification Management. Those are the two basics of the program as far as getting the job done.

Now on the contractor's side, I have a few items I'd like you to help us with. One is to make sure top management is aware of foreign ownership, control, and influence reporting requirements. This requirement is something that's getting emphasis from the Congress. If you become involved in a foreign purchase, or they purchase you, and then after you have three different foreign nationals on your board of directors, you say, "Don't invalidate our clearence," it's a little tough for us not to do something with it. So if you have even the thought that you may become involved in foreign ownership, control and influence, please let us know early.

On adverse information reporting, make those reports to DISCO if you have a problem.

Mr. O'Brien has already mentioned the interview-oriented background investigation. Help us by giving us places to conduct those, and by properly submitting the Personnel Security Questionnaires (PSQs), and then the new release forms we need on the DD49s. Give us assistance. If not, we'll have to reject the forms, and that will just delay the clearances.

I might mention self-inspections. If you do a good self-inspection we don't have to worry about having problems when we come out to your plants because you have corrected all the deficiencies before we get there. Then we cannot even enter into a compliance role. We'd simply enter that "helping" role that we mentioned.

And then the last thing is to properly protect the classified information because that's your job and ours.

Mrs. Joan L. Turner: I'm very proud to be able to participate in this year's seminar. I think that each of us will reap rich benefits from being here. The reason I'm able to attend this year is because you are in my region. We all recognize what this Society has done in the past years to enhance the overall concept of industrial security. Meetings like this, where industry and Government representatives can meet and exchange ideas and opinions with a true spirit of partnership, are one of the essential elements of our program's success.

I want to tell you about some of the responsibilities and functions of a Cognizant Security Office. With regard to the Cognizant Security Office, I represent the New Orleans Region. We have nine; we all operate under the same rules and regulations. I know some of you doubt that statement when you consider some of the varying interpretations that you get from us. And you will see in the near future more standardization of our approach to the protection of classified information in the hands of industry because every effort is being made to assure that we represent the one-face-to-industry concept.

Mr. Dick Williams mentioned the facility clearance and personnel clearance functions of our Cognizant Security Office. I'm going to go into depth on those. I want to mentioned some of the programs that have taken on special emphasis within the Cognizant Security Office within the past year. I'll limit most of our responsibilities to that.

The first is Automatic Data Processing (ADP). Now all Cognizant Security Offices have an ADP specialist on their staff. This ADP specialist also is trained in industrial security, and will work with you and the local Industrial Security Representative in identifying and approving your systems for the processing of classified information.

We all recognize that this is an ever-changing pro-

gram, and it demands all of our attention and special emphasis. If you don't stay in touch with your in-house ADP specialists and monitor them, you'll be very vulnerable to a violation or compromise relating to the processing of classified information on an unapproved system. It's such an important ever-changing element that it's going to be a special topic for discussion later on in the program.

The second is Classification Management (CM). This also is being looked at with renewed interest. Our classification specialists in each office have been given a new mandate to improve the quality of classification specifications. You're going to see more classification specialists visiting you and the user agencies. They're there to help you solve some of your problems. In each Cognizant Office this specialist is there to help you obtain and understand the classification guidance provided by the contracting activity. So don't hesitate to call on them. They can help get the kind of specification that you feel you need to perform on that contract.

Third, we're going to see changes in the International Program. Many of our contractors are getting involved in the international security program. All Cognizant Security Offices either have one specific individual who handles this type of problem or there is a designated individual in our office who handles these complex international programs. So don't hesitate to call and let them help you resolve your problems. In this way we can get more definitive guidance in the international security program. We need this, and we need your support.

The fourth is Education and Training. One of the most essential elements of a good security program is an effective, active educational program for our cleared-contractor employees. We plan to greatly intensify our efforts to provide selective training for contractors and for the user agencies. We plan to reintroduce the old ACO/PCO road show, which was effective in getting to those people that actually create the classification guidance that's provided to you.

I've mentioned only a few of the team members that are able to assist you. Now I want to say a few words about our philosophy toward industrial security inspections. That's the one thing that directly affects all of us.

I want to bring out how we rate out industrial security inspections. We don't give punitive ratings. We actually rate them in order to help us evaluate the contractor and the security posture at his facility. This rating is a better way to assist you in improving your security posture. All of our industrial security representatives have been given at least four mandates of precise tasks that they are supposed to be able to do, and we expect this of them.

The first is to conduct a thorough and comprehensive review during each inspection at each facility. We are working harder to do this. We have been reluctant, and we've had slippages within the past year. Now we're concentrating on spending the time that we feel is necessary in all of our facilities to conduct this type of inspection.

The second is to assist the contractor in developing the measures that are necessary to correct the deficiencis that we've cited.

The third is that when he's there he should take the time to answer any questions that you might have regarding the program.

The fourth is that we sxpect him to produce an administrative product that is our basis for notifying you of the results of our inspection. Each time we leave a contractor's plant, we want to feel that national security has been improved because of our joint efforts in this inspection.

We cannot and you do not want us to do your program for you. We do want you to know that we can give you full assistance in the resolution of any problems regarding the program. We can only accomplish this by establishing a working team relationship. This relationship exists between the Industrial Security Representative and the local contractors. That's the only way we can have an effective program. We must never forget our joint mission is to safeguard classified information. We all recognize there are various ways to achieve this goal. We're there to work with you, to establish and maintain the best and most effective way for your facility.

Now how do we do this? How do we rate our inspections after we come back and write our reports? Mr. Thomas O'Brien discussed a breakdown of the types of inspections that we have done and the precentages, the first one was where there were no deficiencies.

In the last fiscal year we had no deficiencies in 45 percent of our inspections. That means that we did not cite any deficiencies during the course of the inspection. When you think of 45 percent, contractors are doing a pretty good job of having an effective program without deficiencies.

Next is the corrected-on-the-spot rating. This rating will be assigned when no systems deficiencies were identified, and all of the individual deficiencies were corrected before the completion of the inspection. That varies but that's actually what a corrected-on-the-spot inspection should be. Last year 16.9 percent of our total inspection efforts were corrected-on-the-spot-type inspections.

Next is the letter of requirement. This rating is assigned when deficiencies were noted and were not corrected during the inspection, or when there's a systems deficiency that could result in a continued security problem. All deficiencies found during the inspection are cited to you before our leaving or are contained in the letter of requirement to you. This letter of requirement requests an answer to us within 30 days indicating what corrective or preventive actions have been taken. Thirty-six (36) percent of our inspections were letters of requirements last year.

The next one is the major-type inspection. This rating is assigned when systems deficiencies exist that could result in loss or a compromise and that require timely corrective action. Under these conditions and in spite of the on-the-spot corrections, a major rating will be assigned; and the contractor will be required to provide us with written compliance showing what action has been taken to correct the deficiency. Depending on the circumstances, compliance inspection is normally conducted within 30 days. Sometimes this is not necessary on a major inspection evaluation.

This letter of requirement to management is a little bit different in this situation. The letter identifies major deficiencies that have been cited. We also inform top management that if these major deficiencies are not corrected, it could lead to an unsatisfactory security evaluation.

In my region, I go a little bit further. I go the second mile. I've had some experiences with major inspections leading to unsatisfactory. So now I write a personal letter to the top management of these facilities and tell them of my personal concern for their security posture and of the deficiencies that were found, and I request that they give personal support to their program to correct these deficiencies so their security program posture will be at an acceptable level. It's been very effective. At least top management can't say later that they were not aware of the seriousness of such as evaluation.

The next one is the unsatisfactory security evaluation; and because of the seriousness of such an evaluation, the managers need to know. As security officers you must inform the managers that these major deficiencies, if not corrected could lead to that rating. An unsatisfactory security evaluation is a grave concern and requires immediate attention and corrective action. (We had three facilities last year with unsatisfactory evaluations.) This evaluation must involve top management for corrective ation because experience has shown that most unsatisfactory evaluations are a result of the lack of top management involvment in the security program. So the lesson for security officers should be obvious.

In the case of unsatisfactory security evaluations, normally the Director of Industrial Security will visit that facility before our reinspection. On an unsatisfactory evaluation you always have a compliance inspection and a reinspection. We normally visit the facility to help work out a plan of action that will assist the contractor in bringing his security program up to an acceptable level.

For a unsatisfactory evaluation, more forceful letters are used. With each rating, letters get a little more forceful, and this one states that you have been rated unsatisfactory. We tell you, the contractors, and all user agencies that have contracts in that facility at that time that his facility has been rated unsatisfactory. In extreme cases, of

course, the Cognizant Security Office will also tell these user agencies whether or not the classified information in-house is in immediate danger of compromise. If so, they can ask us to retrieve all classified information. Such a rating, if not corrected immediately, can have an adverse effect on a contractor's continued eligibility to perform on any classified contracts.

I've only given you an insight into a few of our responsibilities and functions. I also want to stress that now we are able to assist you in developing a viable industrial security program within your facility. Our industrial security representatives are there to assist you, so don't hesitate to call on your local representative or your local Cognizant Security Office. We work as a team, and that's the only way we can have effective programs in your plant and a total industrial security program.

Ms. Sandra J. Waller: We have been working on the changes to the Industrial Security Manual (ISM), so I will give a brief summary of some of the changes that we expect to make in the ISM. As Mr. Van Cook has said, we are not expecting a lot of changes to the ISM. There will be some changes in the definitions. Some of the ones that will change will be CONFIDENTIAL, the definition for classification authority, classification guide, and the definition of derivative classification. These will be very minor changes, mostly to make the wording agree with the new Executive Order.

The change in the definition of CONFIDENTIAL will be that the word "identifiable" will be deleted. The other changes will be very minor.

There will be one new definition that we expect to put in the ISM. In the draft of the 5200 IR there is a definition for the first time of Carve-Out, and we anticipate adding this definition to the ISM. I'm not going to talk much about Carve-Outs because it's kind of a sore subject with us and because Mr. Irving Boker and I believe Mr. Arthur Fajans will touch on this in the program.

There will be only minor changes to the marking requirements of paragraph 11, of the ISM namely this notation, "Originating Agency's Determination Required," (OADR) will be added.

The most noticeable change in the ISM will be the deletion of a lot of the information, especially in Appendix II on the regrading, downgrading, and declassification portion of the manual. In this appendix, we also plan to include procedures for upgrading of classified information by contractors. Currently, this area is not well covered in the ISM, and this has caused many problems in the past. Because Appendix II will require more change than any other section of the ISM, this will be a good time to include these procedures on upgrading by contractors. We don't acticipate a complete reprint of the ISM. We expect to issue a change package.

We also plan to correct some inconsistencies that appear in portions of the ISM that will be changed because of the Executive Order. We admit there are some problems with the ISM.

Paragraph 11.a on marking paper copies of documents now contains some information that doesn't apply to marking paper copies but to other material. That information will be moved to the proper paragraph and will be put in marking of material other than paper copies. We will also correct the paragraph on marking working papers that now refers to a nonexistent paragraph.

Also, there are a couple of paragraphs in the ISM that refer to another paragraph or several paragraphs. (The ISM, is not on a computer, and we can't push a button and find every reference to every paragraph.) So it is easy to change a paragraph and overlook the fact that the paragraph was referenced in another paragraph; and now you've completely eliminated it, but you didn't eliminate the reference. That covers the changes to the ISM.

We have seen only the draft to the Information Security Oversight Office (ISOO) implementing directive and the draft on the 5200-IR, so there could be additional changes in the final draft. I want to add one more thing on the ISM. It's not at the printers. So we will be a while in getting it to you. However, there are no drastic changes in it, and I think it is an improvement.

Mr. Steven Garfinkel has mentioned the GAO report that was issued by Mr. Irving Boker's office. The GAO report has been mentioned at every meeting I've been to for the last year and a half. It has inspired a lot of us to do something about the

problems we have in classification guidance that has been issued to contractors or, in some instances has not been issued to contractors.

In the Industrial Security Program we have been placing more emphasis on our review of the DD254s that are issued with classified contracts. Our Classification Management (CM) Specialists review all of the DD254s received in the Cognizant Security Office. If they feel that the guidance in that DD254 is not adequate or needs some clarification, they go back to the user agency for additional information. We are encouraging our CM Specialists to act as a go-between for the contractor and the user agency if the contractors are reluctant to go back to the customer. We are encouraging the CM Specialists to make special assistance visits to contractors' facilities to see the DD254 in operation and to give advice and assistance.

We have made some progress in this area since the GAO report, but we still have a long way to go. The problems are not going to be solved overnight. I firmly believe that the contractor has to assist in the preparation of this classification guidance. If they receive guidance that is inadequate, they have to go back to the user agency. Before we can make any great improvements in the classification guidance area, we have to make a real team effort between the contractor and the user agency. This line of communication has to be there before the problems can be solved.

I would like to see a statement included on every DD254 that encourages the user of that form to contact the issuing activity if they experience any difficulty in interpreting the guidance, or in using the guidance, or if they have any recommendations for improvement in the guidance. I don't think item 12 on the DD254, that asks the user to refer all questions to such-and-such a person, is really accomplishing that task.

Mr. Thomas O'Brien has mentioned changes in the Cognizant Security Offices. We are currently putting out the latest Industrial Security Letter (ISL). In this ISL the changes to the Cognizant Security Offices are all listed including their new telephone number, and a map of the area. There's also information on Executive Order 12356.

Some may not know that we are reviving the Industrial Security Bulletin (ISB). This is the document that's issued to the user agencies. It's not issued to the contractors. This is a good way for us to let the user agencies know of the problems we are experiencing with their guidance or to help them with guidance on the problems we're haveing. We had quite a bit of information in there on classification management — DD254s which are not properly prepared, request for safeguarding ability, and so on. All of our CM Specialists are listed in this ISB as well as the changes to the Cognizant Offices. There are two documents that will have those changes in them.

I have one other thing. In the March 1982 issue of American Society for Industrial Security ASIS' *Security Management* magazine, has an article entitled "Classification Management —The Keystone of Industrial Security." By Mr. Thomas O'Brien. We have received some very good comments on this article, and one user agency has asked ASIS for permission to reprint it in one of their security education bulletins. There is some good information in it, if you can get a copy.

Mr. O'Brien: Now we are open to any questions that you may have.

Question: Sometime back we asked what to do when at the end of a contract, retention requests come in saying they're retaining information under the contract clauses that authorized retention of certain materials that are required for audit. Someone was going to find out whether or not this included classified documents. User agencies are not certain of this. Is there any way you can explain that?

Mr. Williams: The question relates to portions of the contract. They have two things. They have warranty clauses, and you have to maintain the records under warranty. You have to maintain certain accounting records, and sometime those involve classified material. My opinion would be that if the contract provides for it, then the retention should be authorized because if the contract specifically states that an item must be retained by the contractor and the contractor is ordered to retain it for the benefit of the Government, then certainly that ought to constitute the authority to keep that particular item. I know this is true on certain Navy contracts with relationship to ships'

plans and warranty information on weapon systems. Those are classified items. They are covered in the basic contract, and they specifically state that the contractor is required to keep them for a set period of time. If there is a question that the Cognizant Office has when we're doing our inspections, then we would go back to the user agency and say, "When you wrote that contract, did you really want them to keep those items for that period of time"? That is true on Navy vessels, and it's true on weapon systems.

What I'm saying is, if the contract provides for the requirements for the contractor to retain the records, then, yes, it would be provided for as far as authority to keep it under the retention requirement. Now if this is a confusing matter, we can get together an ISL item on that. I think that would be a good subject. Would that help you out?

Mr. O'Brien: Let me add one additional word. The philosophy is that: for a contractor to have classified information there be a contractual relationship, so you'd only have classified material in your custody if it's necessary in connection with the contract performance. Now contract performance is interpreted to include what has to occur after the contract has been accomplished.

The contracting officer must authorize retention of any material that you are to keep after you have completed all the normal contract obligations, and it's between you and him in a sense, and you have to identify what it is that you have to retain and why. We have specifically provided, as a policy matter, that the information that must be retained is for subsequent audit purposes. Now it's up to you to say, "Yes, we have this kind of data that may be subject to a GAO audit or a (DCAA) audit," or whatever. If the contracting officer comes back to you and disallows that; and you feel you have a good case, then we're willing to mediate, that kind of a thing. We'll come in and work with you and your contracting officer and make sure that there's no misunderstanding. If you really need it, the retention will be authorized. But in the last analysis, it's your responsibility to make the case that indeed you need it for this purpose.

Ms. Waller: Weren't you talking about the retention requirements, the military records retention clause in the contract itself, that says the contractor can retain certain documents?

Response: Under paragraph 5(m) of the ISM, it says "essential records." Sometimes the contractor looks at this and says, "I need it for essential records." We're supposed to know — let's say it's a small R&D contractor — whether they need the final report. I understand for audit that you may not need the final report, but that it's the financial records that are needed.

Mr. O'Brien: Right. It's more financial kinds of data that would be follow-up from a cost standpoint.

Question: I'll address this to Mrs. Turner. Our facility had a two-day inspection recently. During the preliminary exit debrief with the security supervisor, the inspector said there was a new trend coming out of DIS. In the past, deficiencies that were found to be immediately corrected-on-the-spot — those kinds of things that were mutually agreed between the security supervisor and the inspecting representative — would not be necessarily cited in a letter. The inspector said that there would be (and I quote) "no more Mr. Nice Guy," and that anything that was seen would no longer be mutually agreed upon and would be listed in a letter. Is there any validity to this new trend?

Ms. Turner: In our region, we consider corrected-on-the-spot to mean that the deficiency was corrected before the completion of the inspection, by the time of the debriefing; and then it normally would *not* be cited. The promise, "I'll do it," and then we come back later and it's not done, cannot be accepted as corrected-on-the-spot. It has to be completed before the completion of the inspection. That's the way we interpret it. Also, in our letter back to the facility on the corrected-on-the-spot, we bring to your attention that the Security Officer is aware of those items that were corrected-on-the-spot. But they are not identified as deficiencies in our letter of requirement.

Response: I realize that, but he said it will be mentioned subject by subject.

Ms. Turner: I don't know the new trend.

Mr. O'Brien: There is no new policy. We still are Mr. Nice Guy.

Ms. Turner: I'm not in the new trend apparently because we've not been directed to cite everything whether it was corrected-on-the-spot or not. I've not been told that.

Mr. Williams: Let me address that. I was the Director of Washington when the region started. I found a variance of operational policy. Some of you occasionally get the idea this happens from region to region. I know there must be some instances of that, but I haven't observed any.

But from field office to field office and from Industrial Security Representative to Industrial Security Representative there are differences because there are differences in people. If there wasn't a problem with people, we wouldn't have any problems with the DIS; and we all realize that.

In Washington I found no uniform application of inspection grading standards. I found that we had Industrial Security Representatives who would say, "If you promise you'll correct it, then I'll accept that," and that's what you're talking about. Then there were other inspectors who said, "You must finish correcting it within the next five minutes, or I don't accept it as a corrected-on-the-spot."

What was put out to the Industrial Security Representatives was that if the deficiency was corrected before the completion of the inspection, then that was a corrected-on-the-spot. If it was not completed at the completion of the inspection, then it was a written deficiency.

There was one thing put out that does not amend that policy but gives some latitude to the Industrial Security Representative. It says that if you have a good, established rapport with the contractor, and in your mind that deficiency is corrected before the letter of requirements is put out, and you're willing to put your reputation as an Industrial Security Representatice on the line accepting that contractor's corrective action, then I'll accept that position.

In this instance you may have had a turnover of inspectors. It may have been a different inspector or one that had allowed the deficiency to be corrected-on-the-spot, and at the next inspection the same deficiency showed up again. This happens a lot of times. In other words, the singular briefing statement, the 482, was corrected; but there were three others in the next inspection that were not corrected. If they see that type of trend developing, the requirements would be to make sure it's corrected before they leave. These things would occur between the contractor and the Industrial Security Representative. Based on the judgement of the Industrial Security Representative and the past performance of the contractor, then a decision would be made whether or not it would be called corrected-on-the-spot.

DoD/INDUSTRIAL PANEL PRESENTATION ON CLASSIFIED MANAGEMENT PROBLEMS AND SOLUTION

Eugene Dunsmore (Moderator)
Classification Management Chief
Lockheed Missiles and Space Company, Inc.

Arthur Fajans
Directorate of Information Security
Office of the Deputy Under Secretary of Defense (Policy)

Joseph A. Grau
Office of the Assistant Chief of Staff for Intelligence
Headquarters, Department of the Army

Gerald Berkin
Head of Classification Management
Security of Military Information Division
Office of the Chief of Naval Operations

George Paseur
Director of Information Security
Department of the Air Force

Eugene Dunsmore: First we should establish what this panel presentation is not. Our purpose is not to tell you what we feel are the major problems in classification management within industry. The panel make-up is not to imply that the Government is more aware of classification management problems than industry. We are not going to allow

you the luxury of not being involved in this presentation.

Let me introduce the members of the panel: Mr. Arthur Fajans, The Chief of the Requirements and Evaluation Branch of the Directorate of Information Security, Office of the Deputy Undersecretary of Defense for Policy; Mr. Joseph Grau, Security Specialist with the Counterintelligence Directorate, Office of the Assistant Chief of Staff for Intelligence, Headquarters, Department of the Army; Mr. Gerald Berkin, Head, Classification Management Branch, Security of Military Intelligence Division, Office of the Chief of Naval Operations; and Mr. George Paseur, Director of Information Security, Headquarters, Department of the Air Force.

After several weeks of telephone discussions with NCMS area coordinators, chapter chairpersons, and individual members, I solicited the concerns that are being discussed within your area, chapters, and companies that should be addressed at this seminar. Your responses were loud, clear, numerous, and quite challenging. Those responses were concolidated into subjects and then double checked with other scheduled speakers to try to eliminate any duplication and to insure that the subjects that you wanted were going to be covered at this seminar.

So, you are already involved. This is your presentation. We are responding to your expressed concerns. Listen carefully; take notes. And after you've heard from all of the panel members, we will call for further discussion and questions from you on these topics

With the recent proliferation of Special Access Requirements (SARS) Sensitive Compartmented Information (SCI), Operation Security (OPSEC), and Carve-Outs in Government programs, what is their role in relationship to the overall Industrial Security Program? How are they created? What are the guidelines? What effect will they have on the future of the Industrial Security Program and Classification Management? These questions will be discussed by Mr. Arthur Fajans.

Mr. Arthur Fajans: I've been asked to discuss the role of Spacial Access and Carve-out Programs and their relationship to the overall Industrial Security Program. How many of you are having problems with Carve-out Programs? That's what I was afraid of, and I don't think you all are being honest. I think there are many more hands out there, or perhaps you didn't want to let people know that you're associated with a Carve-out Program.

The origin of the term Carve-out has apparently been lost in antiquity. Since the term was not clearly defined, it's taken on different interpretations. It also seemed to take on differing aspects, different from those normally associated with Special Access Program, and has received ever-widening acceptance.

The basic concept behind the establishment of Carve-outs is that there are certain classified contracts or portions thereof which are so sensitive that special security procedures must be created. Among them, the retention of security inspection responsibility by the contracting activity and inspections conducted in accordance with the Industrial Secruity Program are carved out.

To set historical prespective for this problem, let me quote from a 1971 memorandum. "OSD has been working on a program to eliminate special access programs and has asked the departments and agencies to identify all such programs and justify those they feel a need to continue. Even though the problem is not completely solved as yet, the policy people are working on it." That was 1971 when it was estimated in a somewhat imprecise way that there were some 135 Carve-out Programs. In 1973 this number increased to a little over 200. By 1977 it had grown further. Currently, we believed it to be in excess of over 800. The problem is not completely solved, and the policy people are working on it.

First, Special Access Programs cannot be addressed mearly from the DoD standpoint because many of them are national in origin, are based on requirements and needs stemming from national intelligence decisions and are combinations of intelligence collection, operations, and research and development. Of the in excess of 800 programs that we believe are currently in existence, over 500 of these are under the coognizant of the Central Intelligence Agency or the National Secur-

ity Agency. The remainder are under defense program manager cognizant, and many of those are in the defense intelligence community.

Executive Order 12356 does not differ substantially from Executive Order 12065 in terms of the requirements for the establishment of Special Access Programs. As Mr. Irving Boker pointed out to you, 12356 says a little less, but the requirements have not changed and will not change in terms of implementation of the DoD 5200.1R Regulation. The Regulation will differ in its provisions concerning Carve-out Program.

It is important to maintain the distinction between a Special Access Program and Carve-out Contracts. The major problem attendant to a Carve-out Contract seems to stem from project managers outside the intelligence community who feel that information concerning their programs must be protected from established industrial support mechanisms. However, they fail to realize that exclusion of the Defense Investigative Service (DIS) from inspection responsibility requires them to establish their own security structure.

To begin treating this problem, 5200.1R will require, in addition to existing Special Access Program provisions, that each DoD component will establish a single point of contact for security control and administration of all Special Access Programs established or existing in the component. The use of Carve-out Contracts that relieve the DIS from inspection responsibility is prohibited unless such contracts are in support of a Special Access Program approved and administered in accordance with the provisions of the Regulation.

Approval to establish a Carve-out Contract must be requested from the Secretary of the military department or his designee, or in the case of other DoD components, from the Deputy Undersecretary of Defense for Policy, General Stilwell. Approved Carve-out Contracts shall assure the support necessary for the requisite protection of classified information involved. This support shall be specified through a system of controls that shall provide for a written security plan, Carve-out Contract procedures, a central office of record, and single point-of-contact for security control and administration. Components other than the military departments shall submit approporate rationale and security plans along with requests for approval to the Deputy Undersecretary of Defense for Policy.

To complete the picture, there will be a definition of Carve-out in 5200.1R: A classified contract issued in connection with an approved Special Access Program in which the DIS has been relieved of inspection responsibility under the Defense Industrial Security Program. These changes will be coordinated with and integrated into the Industrial Security Regulation (ISR), and it is anticipated that the ISR will contain specific criteria for the establishmenty of Carve-out Contracts within Special Access Programs.

Finally, I want to report some progress in standardizing inspection procedures and insuring reciprocal inspection results. Agreement has been obtained among the Defense Intelligence Agency, the Army, Navy, and Air Force, to accept each other's inspection results in some cases. However, there still remains an inherent reluctance on the part of the Intelligence Agencies to let anyone else scrutinize their activities, based at least theoretically on the concept of need-to-know. So for the moment efforts are being concentrated on organizing the regulatory procedures and directing them toward the nonintelligence area, believing that success in these area will begin to draw things together. General Stilwell has endorsed this phase approach to what he recognizes as a very significant problem.

For many years in the late 1960s, I worked for theDefense Intelligence Agency (DIA). At that time we used to wear badges and they had numbers on them — 1, 2, 3, 4, 5, 6. Two (2) stood for access to CONFIDENTIAL; 3, access to SECRET; 4, access to TOP SECRET. Five (5) was for SPECIAL COMPARTMENT INFORMATION; And 6 was another SPECIAL COMPATMENTED INFORMATION access. I observed in that environment that when you met for a meeting, there was immediate observation of the badge and relationships immediately were set up. If you had a 6 and he had a 4, you knew that there were certain things that he just couldn't know. They almost were not access badges. They were badges of honor, prestige, and prerequisite. Back in the later 1960s information was power. In the 1980s nothing has changed to reinterpret this old traditional axiom.

Carve-out Programs can become badges of honor, prestige, and prerequisite. We, in Government and in industry, should do what we can to prevent that interpretation. I believe there is a valid reason for Special Access. There's a valid reason for Carve-outs. Let's try to keep those systems within those valid boundaries.

Mr. Dunsmore: What are the differences in approach to writing classification guidance for research and development contracts (sometimes seen by industry as minimal directions) and production or operational contracts (sometimes seen as prolific direction) in terms of an overall major program? What is the evolutionary cycle of classification guidance. Mr. Joseph Grau will discuss these topics.

Mr. Joseph Grau: Let me give you some idea of the perspective from which I look at classification guidance. I have spent a year as the classification management officer for one of the Army's major development and readiness commands, the and development and material management folks for electronic equipment. I was heavily involved with the preparation of guidance and worked with the people who actually prepared the guidance.

Then I came to the Pentagon and spent two years in the security review function in the Office of the Assistant Chief of Staff Intelligence (ACSI) of the Army where I was a heavy user of guides. I was in the same position that most of you find yourselves in — trying to figure out what they actually mean. Then I moved out of that job and for the past year and a half I've had very little close involvement with guidance which means I have a bit of a detached prespective on it.

Where does classification guidance come from? What happens when classification guidance is initially developed for a project? First of all, somebody figures out that we need a guide. It could be a new project, a new program, a new idea that someone is going to begin working with; and they realize that classification guidance is necessary. Unfortunately, in many cases it's not a brand new program. It's a program that's been around for a while in someone's laboratory, office, or mind; and the realization is that we need classification guidance. They know the system. They know the details of what the project is going to involve.

What do the security people do? Traditionally the security people have prodded, they've tried to assist, and they've reviewed the product. What's the problem is that too often the security input to the classification guide has been superficial. The security people seldom know the technical ins and outs of the project. Often they don't have time to learn. The security people have a body of expertise, in classification management. To make constructive contributions to a guide, they need somebody of knowledge on the technical aspects of the system.

As I have said about security education, we all too often don't have the time, money, or the people to do everything we want to do. At times what suffers, in the classification management field from our lack of resources, is that the security people do not have the luxury to bring themselves up to speed on the technical aspects of the project they're working with. Quality of guidance, in my opinion, is a function of the security expertise that's available at the preparing activity; and the availability of the pople who have that expertise to work with the technical folks on the guidance. What we need is a real honest team approach to classification guidance.

We are thinking in Army right now of a possibility of a murder board approach to classification guidance. It's just one thing we're looking at. Don't go back to The Department of the Army Readiness Command (DARCOM) and say, "We're going to set up murder boards."

The reviews by security people of finished products need to be substantive. Too many times the security people check whether somebody has R-E-V-I-E-W or R-E-V-W, or they start adding up dates (which mercifully we won't have to do anymore) to make sure you didn't go one day over 20 years, that sort of thing — format oriented. We have to get away from that, and I think we are getting away from it. In the past few years I have seen a monumental improvement in the theologic of Army classification guidance, and I'm speaking from the user's aspect the guy who had to sit there and read the things and figure out what they mean.

Now you have the guide. What happens to it from there? How does guidance evolve? We have biennial reviews — to review and up-date your guide. Biennial reviews are a *pro forma* response to a regulatory requirement. I seriously doubt from my experience whether much substantive decision making about classification is done at the time of the biennial review. I'm not saying we shouldn't have them because before we had the annual review/biennial review requirements, you would open your safe drawer and find one of these old dogs that had been laying in there since 1962 and nobody had touched it since. By then, the organization had reorganized 11 times, and you couldn't figure out where the guy was who knew what the rationale was behind the original decisions. I don't think biennial reviews are the times when substantive decision making is done.

Real change in guidance occurs in response to user input, and it occurs in response to external influences — happenings out in the real world and input from people who are trying to use the guidance.

What are problems with this? The problems are that we talk about planning classification into the future. The DoD handbook, an excellent product, talks about looking at stages of development of a project and trying to preplan the classification needs of the project ahead of time, which in theory is a marvelous concept. As far as it can be executed, it's fine. But evolution in project development is only one consideration in classsification changes. It occurs simultaneously with changes in the state of the art. And if you could determine at the time you originally prepared a guide what the state of the art was going to be in five years, you'd be there already; so you can't very well preplan that, International political development can have an effect on guidance particularly when we need to change guidance in response to international occurrences in international programs we're involved in. Programmatic changes occur and funds go from 50 megabucks to 10 megabucks, and you've got to restructure your system. And disclosures leave an effect.

Imagine if you will — and I have never seen the classification guidance for this particular project — but let's say that at the time for its inception some people sat down and made a very good, thoughtful, logical effort to pre-plan classification guidance for this particular project. Cast yourself back to about a year and a half ago; put yourself in the position of the action officer for the classification guide, and imagine what your feelings would be when you turn on your television set. The project I'm refering to is the Stealth aircraft. These are the kinds of problems we face.

What does this do to us as security people? It makes it awfully difficult for us to convince the technical people and some of our fellow security that it's worthwhile trying to pre-plan for evolution of guidance through the development and production phases of a project.

What do we do about it? The old saw: we need to improve our management of the process. I think this is true. Classification management has to be truly a management process which means that you try to control your future. That's what management means. It should encompass the future as well as the present to the maximum extent possible. In the Army we're considering several intitiatives to try to assist in making this more of a reality; and they're just in the wild theory stage.

However, no matter how much we try to preplan guidance; and say that at the time of production, XYZ component will become unclassified and at the time we load in the operational data, ABC component will become SECRET; no matter how much we try to do this thing and try to control our future, the evolution of classification guidance, the changes that you find being made to guides, are going to continue to be substantially reactive. This means that the preparers, the people responsible for the guidance, need quality input from the users of the guidance.

In the past few years I have seen, in the Army and in our relationships with the other services and some other Defense and Non-Defense agencies, that interaction between users and preparers has improved. We as users have begun talking more to preparers in other departments and agencies. They as users have begun talking to our preparers more, and this is terrific. But industry

has a very important role to play in the evolution of classification guidance.

When someone tells me that classification guidance does not meet the needs of industry for a particular product, my first question is, *"How have you enunciated those needs to the user agency?"* Thats really my second question. My first question is, *"Have* you enunciated those needs to the user agency?"

And allow me to voice one of my personal prejudices. Industry has to become aware, we have to convince them, that the preception some people have that challenging or questioning the classification guidance they receive, somehow is going to make them less competitive for some future contract is baloney — absolute baloney. In my 12 years in the Government (several of them intimately involved with classification guidance) I have never seen, heard, or even suspected one single incident of this. Yet when someone challenges development, unfortunately it's all too common to hear this old saw resurrected.

If this is a cop-out for failure to participate in the classification management process, be advised that many of us in Government meet it with a good bit of suspicion. If it's an honest concern — and I believe that for some people it is, if not for all people — we need to talk to each other and eliminate it.

The quality of classification guidance, in any stage of a program, can best be judged where it's applied — by users of the guidance in Government or in industry. If guidance is to cover what should be covered, as it should be covered, intelligently, effectively, user feed-back is essential. We need to promote a spirit of cooperation between users and preparers and at all costs avoid an adversary relationship. Contributions to the effort and constructive criticism, no matter what their source, be it from other Government folks or from industry folks, are welcomed by people who are interested in doing the job right. I stress constructive criticism.

It's the old story that we hear at these sessions so often. I believe it, and I hope that you believe it. When it comes to classification management, we truly do need to work together.

Mr. Dunsmore: As participants in the industrial security program, contractors are required to establish a basic security program. As long as classification requirements established by the Government are up-front, provisions for them can be made in our bid and proposal process. What are the types of classification requirements or recent security changes that contractors should be aware of as having dollar impact on his basic security program? And what is the Government's policy for consideration of these costs? Mr. Gerald Berkin will address these areas.

Gerald Berkin : When Mr. Eugene Dunsmore asked me to talk on this subject I assumed that if the question was posed, there must be a problem. So I had the major Navy commands surveyed to see what problem there was, if this had come about before, and if we had heard any rumblings from industry that we weren't quite forthright in providing information in the bidding process so that industry representatives can sensibly prepare their bids with full consideration of the special considerations that might modify or expand the basic security program. So let's look into this kind of problem because the Navy commands that I spoke with didn't recall that there was a problem. But if people feel there is a problem, then something is really wrong. How does one dissect this kind of issue to see where the problem is and what can we do about it?

Perhaps the Government contracting officers or the technical people who prepare the specifications for contracts don't bring security staff in early enough so security implications — whether peculiar, standard, or whatever — are known in the precontract discussions that take place. That's a possibility. In the laboratories that I was associated with in the Navy, I don't think we had that problem. But that is a possibility.

Perhaps contractors face the same problem. Your marketing people or your sales types, in their zeal to nail down a contract, may not discuss these kinds of things with security staff early enough so you can make your marketing people and management people fully aware of the dollar impact of some of these odd security requirements of Government OPSEC, ADP, SCI, Carve Outs and all the other peculiarities of this business. I don't know,

but that seems a logical kind of thought.

There are a lot of small companies that have problems like this too. Small companies may not have a large security staff available to them with a great deal of expertise, so the company itself is unaware of the dollar impact of some of the security requirements that are laid out for them, so they would seriously underbid and then feel they'd been had by the government. I don't know. That also seems a logical possibility.

So if there is a problem, I imagine the problem is one of competent staff being brought in at the proper time and communication between the Government representatives and the industry representatives, because the security requirements for these special kinds of programs are not that arcane. They're laid out in a variety of manuals and in a variety of other places, and these things generally are known in the precontract discussions and conversations.

Of course, there's always the possibility that in the midst of a contract you can get changing security requirements based on changing operational requirements or changing threat information that's known to the Government and is not known to industry for a variety of reasons, most of them because they go beyond the company's need to know for that specific thing that they're going to make or whatever they're going to do, and in such a case is a change of contract, the Government is willing to talk to industry representatives and possibly amend the contract.

So if there is a dollar impact in the bidding process, it's incumbent upon industry staff to be thoroughly and completly familiar with the security requirements governing any one of these areas, Automatic Data Processing (ADP) protection, Operation Security (OPSEC), or whatever. Industry representatives must ask a lot of questions of their Government counterparts. What do you really want? What's going to show up on that 254? And then industry must be able to translate those requirements, some words a bit more precisely than others perhaps, into the dollar costs so that their bid can reflect the cost to the company to do this thing. Because once that's done, all of this is an agreement between adults. It's a contract. And the contract must be precise if you don't want any problems, and one must sbide by the terms of the contract.

If one party to that contract is ignorant of some of the implications or problems, that's an unfortunate circumstance. It's unfair to cry to the Government later that you've been had. If the Government does not provide the required information up-front, that's terribly unfair to industry. But you must be able to query the Government and draw this information out so you can make a sensible bid that won't hurt your company economically.

Perhaps, industry doesn't know the requirement or doesn't ask enough questions to get the information they need. So rather than say I didn't find any problem because the Navy commands that I queried said: "You mean this is really a difficulty? No one's brought that to our attention. We provide 254s. We have precontract discussions. We didn't know there was that much difficulty." So apparently you do have some problem. Again, I say that your security staff must be thoroughly knowledgeable of the basic requirements, minimum standards, or whatever other standards relate to the protection of information in these certain circumstances. If you don't, how can you enter into a contract? How can you enter into a contract? How can you possibly estimate costs? You must obtain this information from the Government. If it's not readily available you must demand it or else you can't bid. Or if you bid and you accept that, it is a legal contract. You're bound by it. I guess you can go back to the Government and say, "Hey, I want to renegotiate that," but that's not right.

So I hope I've covered some of the logical possibilities where difficulty may arise for industry. And insofar as the Department of the Navy is concerned, I can assure you it's not the intent of the Department of the Navy to take anybody because the relationship with industry has always been a close one, and industry supports the Department of Defense's objectives and the Department of the Navy's objectives. The last thing in the world we want to do is have an adversarial position with industry.

If you do have a problem in this area, you must

make certain your security staff know all of these requirements. You must make certain that you're cranked into the contracting process with your marketing and management staff early enough so you can advise them. Don't put the onus on Government. If the Government is remiss in not providing the information, you must obtain that information. If you need help, the DIS people are at your disposal to provide whatever counsel and guidance you need as independent arbiters not related to a specific service or military department. ment. You can get help anywhere — from my office, Mr. Maynard Anderson's office, anyplace — as to what these strandards are.

Again, it gets back to education and training for security staff. And this has always been, if I might digress for a moment, an interesting point to me. It's essential that all Government and industrial people receive some kind of formal training in the security business.

If you talk to five people in security, you'll get five different definitions of what security is. And you'll find the backgrounds are as varied as the faces you're talking to. Everyone speaks from a set of biases or opinions that may not match yours.

It's essential that we all sing from the same sheet of music, that we all know what we're talking about, and things generally will work out all right. There will always be difficulty; but as long as people talk with one another, and you're dealing with fellow professionals, we won't have any kinds of problems.

I don't know if I've solved anything for you, and I certainly haven't tried to whitewash anything. I really was unable to uncover, and none was made known to me, in the Department of the Navy and problems of the type that were brought to my attention. And I merely laid out for you some of the possibilities where difficulty may arise. I hope that's been of some help to you. Again, my office in the Navy stands ready to help anyone who has a problem in this area.

Mr. Dunsmore: DD 254s sometimes reference military service regulations that, as seen by industry, have no contractor involvement. Example: Air Force Regulation 207-1 — the Air Force Physical Security Program; Air Force Regulation 55-30 — Operation Security. These are difficult to obtain. Why are they listed? Is industry required to ascertain and state their non-applicability? Sometimes when we obtain copies of these regulations, interesting questions develop such as "What is system security engineering? How is it handled in the Air Force? By engineers?" Is there something for classification management in application of this technique? George Paseur discusses these questions.

George Paseur: The DD Form 254 seemed like an easy subject to discuss because I didn't think we had a problem in the Air Force and probably not in the rest of the Defense Department, with referencing regulations or guides that were not available to a contractor. But since several people have brought it up, I decided to check into it.

In talking with some of my friends in industry and some people in the Army and Navy, I came up with what apparently is the case. In many instances preparers of DD 254s are referencing Air Force regulations or classification guides and not providing those referenced documents to the contractor for use. What do you do when you get into a situation of this type? Should you go back and request the documents that are referenced? I think the answer to that is simple. Obviously you should.

If you are given guidance or guidance is referenced in the DD 254 that is not avalable to you, obviously you should ask for it. The question is whether it is your responsibility to determine the applicability of this referenced document to the particular contract? I think that's a joint responsibility.

First, it is seldom necessary — and in the Air Force we try to keep it from ever happening. Obviously, we're not succeeding. In the Air Force we do not want any regulation or classification guide referenced in a DD 254 unless the full regulation or the full classification guide applies to the contract. We want our preparers of DD 254s to extract the information that applies specifically to the contract that the DD 254 applies to and provide the guidance in a direct and specific way to the contractor who will be performing on the contract.

When I found that we *do* have a problem in the Air Force, I immediately took some action. I enjoyed very much Mr. Joseph Grau's presentation and his approach to security education. I think his ideas are excellent, and they are approaches we could all benefit from if we would follow them. But the thing that really concerns me is motivation.

I issued the guidance to the people to not include references; or if you have to reference a classification guide or a regulation in a DD 254, if it is determined to be appropriate, then provide that referenced document to the contractor. But how do you motivate people to do that?

I can issue the message. I can get the information to the security specialist. I can get it to the project officer or the project manager who's working the program. I don't think it's a malicious effort or intent on the part of the preparer to make things difficult for you. I think it's just like Mr. Irving Boker who quoted acronyms that I found difficult to follow after a point, that we very often get ourselves into a situation where we say, "Everybody's going to understand what I'm saying." This applies to everyone.

I would encourage those of you in the industry side of the business, if you do receive the DD 254, whether it's Army, Navy, or Air Force, or whoever, and a document is referenced as required or providing guidance for you in the security area, go back to the preparer of the DD 254 and ask for that regulation. At least that will insure that the person takes a look at it and makes a determination as to whether it's required or not. You have two types of situations here: One is an unclassified referenced document; the other is a classified referenced document.

My office is responsible for nuclear classification for the Air Force. We write the Nuclear Weapons Classification Guide for the Air Force. Many times contracts or DD 254s will reference our security classification guide which is SECRET. Sometimes we'll find one that references the DoE/DoD Nuclear Weapons Classification Guide CG-W-4 which is SECRET and CNWDI as Mr. Arthur Fajans discussed earlier which requires a special access authorization just to see the classification guide.

What we want and what I think you want, is for the preparer of that DD 254 to extract the information from that guide and keep it on an unclassified basis if at all possible and provide you with the data you need in an easily understandable form rather than referencing a 150-page regulation or 150-page classification guide when your contract only relates to two sentences in the guide.

I have no answers for you. I don't know how we'd solve the problem. I can tell you we are going to work on it in the Air Force, and I'm sure that Army, Navy, and the other agencies would do the same. If you are not getting the guidance or are not getting the cooperation from the project managers or the security people who are involved in preparing the DD 254s, i encourage you, as I have in the past, to contact me or the other service representatives as appropriate to get the assistance that you need.

We can get you the assistance. We can bring to bear the necessary influence to get the people who are suppose to be doing the job to do the job.. I guess that's as easy as I can say it. Are there any questions?

Question: You mentioned several times Air Force regulations and classification guides being referred to in the DD Form 254. Are you making any particular distinction between an Air Force regulation and a classification guide? And if so, what distinction?

Mr. Paseur: Some Air Force classification guides are Air Force regulations. For example, Air Force Regulation AFR-20542 is the electromagnetic pulse classification guide. That's a regulation, but it's also a guide.

Regardless of whether it is a classification guide or a regulation, you should not have to leaf through a 250-page classification guide when all you need in that guide is covered on one page. The guidance should be extracted and provided.

Question: My question is, are you distinguishing between a classification guide referred to in a DD Form 254 and an Air Force regulation which is not a classification, which is a regulation, but is not defining elements of information with respect to the classification?

Mr. Paseur: No, the principles are the same. The principles are identical. The guidance that you should be provided is the guidance you require. It doesn't make any difference whether it's in a regulation or in a classification guide..

Comment: What I'm trying to ascertain is this. If you are referencing an Air Force regulation which indicates what information is classified and to what degree and for what period of time, I accept this. Bur if you are referencing in the DD Form 254 an Air Force regulation that does not indicate what elements of information are classified or to what period of time or to what level, then we're talking about something which should not be included in the DD Form 254 in the first place. That's my point.

Mr. Paseur: That's true. If they're going to apply to you in the performance of the contract, they should be made part of the contract if they involve other things. Yes, you're absolutely right. I understand what you're saying now.

Comment: An example is the citing of 205-1 as a compliance document for us. We have the Industrial Security Manual which is a counterpart of that, and we have that cited on occasion.

Mr. Paseur: That's a related issue. We have a lot of contracts that the Air Force elects to exercise security supervision and inspection over, especially in the overseas areas. We have no real choice there under the current guidelines. In many of those cases where the contractor operates, we'll have a military person at one desk, and a civil service guy at the next desk, and a contractor at the next desk — a small internal type operation. We write special security requirements into those contracts, and many times the contractor does comply with service directives. It's more appropriate for them to comply with service directives than to set up an industrial security program for a one-man operation on a consulting-type basis in an in-house type operation in the intelligence shop at Lindsay Air Force Station in Wiesbaden, Germany or something like that.

Comment: I'd like to make one more comment. Currently in 5200.1R there's a requirement with regard to the provisions of security classification guides that the guide should contain not only the information that is to be protected and at what level and so on, but there's also a requirement that says that guidance should be provided on how it's to be safeguarded or under the provisions of 5200.1R it will be marked thus and such. Now it's possible for that reason that many guides may refer to one of the supplemental regulations of 5200.1R. That kind of provision that requires instruction on how to mark in accordance with the regulation is being deleted from the current 5200.1R, so it's possible that there will be no need to reference supplementing regulations in the services.

Mr. Dunsmore: We told you that your questions and your concerns were very challenging for us. I believe this panel has been up to the task of answering those concerns. Are there further comments or questions on these selected topics?

Question: I have one to Mr. Arthur Fajans' comments this morning. With the proliferation of commercial-activity-type contracts on bases, do you see a proliferation of Carve-outs where the in-house contractor who's living on your base will be required to comply with provisions for example, the Navy Security Manual, the Command Security Manual and the Industrial Security Manual (ISM)? There's another part to the question.

The other part is, are you aware of any policy being developed — call it innovative facility clearance — for example, where the headquarters of the company is downtown, and the officers, owners, directors, and executives may not need to have a clearance, but their people operating our graphic art shop would?

Mr. Fajans: I can only give this kind of response; and if it's not satisfactory, we'll talk some more. There's obviously a problem with Carve-out Contracts, and it's not necessarily a problem of providing sufficiant safeguards for the information. I think that's being done. The problem is that some Carve-out Programs are being created where they're not necessary, especially in the nonintelligence area. So Mr. Maynard Anderson is talking the phase approach of trying to get a handle on Special Access Programs and their relationship to Carve-out Programs; and he is taking a regulatory approach

by identifying single points of contact, single points of accountability within Defense and in the military departments; and he is requiring that all Carve-out Programs be associated with Special Access Programs that have been approved.

The Executive Order still requires approval of Special Access Programs by agency heads. Obviously, some Carve-out Contracts are being authorized by officials who should not be authorizing them. Once this regulatory approach is taken and has some degree of success, and we can identify what contracts are out there, how they are being applied, and what their security plans are, then we can correct this problem. It's not going to be corrected overnight, and I don't want to leave the impression that we have solved the problem by a wonderful wave of the regulatory hand. But I think that this is a very important step that will appear in the new regulation and in the Industrial Security Regulation and the ISM.

Comment: The Industrial Security Regulation in paragraph 108 has provisions for the commander of an installation to make a decision. The decision he makes is either to allow the inspection to be conducted by an Industrial Security Representative as one of those normal things that fall under DIS, or he makes a decision to do his own inspection. When he does that, he does not release the cognizance of the facility. It still belongs to the region that has cognizance over that territory.

What happens is, he assumes the responsiblity to perform that inspection. It's not a Carve-out in the context of 5200.1R, and it's not in the ISM yet of course. You, the contractors, may appear to be a Carve-out because the DIS Inspector does not come in and do the inspection. However, it is not a Carve-out within the context of the loose definition we're using as Carveouts. You'll see more of this as we move on to installations.

We have installations right now that change because they are vessels. As long as they're attached to a pier, they're under our cognizance; if they go out in the ocean, they belong to the Navy. So we have a lot of very unique situations. But they're not *per se* Carve-outs within the definition that we're talking about and have been discussing as Carve-outs. Does that answer your question?

Response: Yes, it does.

Question: I assume that when you're using the term Carve-out, you're talking about it solely in the context of some special access.

Response: That's correct.

Comment: Eighteen years ago a little handful of people sitting aroung the conference room all agreed that we need better classification guidance. This morning I saw more hands held up than I've seen in any other meeting, and they said they were not getting the classification guidance that they needed. Have any of you professionals created a DD 254 to hand to your contracting officer to give back to you? How many of you have done that? That isn't near enough of the people that held up their hands earlier. I'd like to emphasize Mr. Joseph Grau's parting remark. God helps those that help themselves.

Question: Does anybody know what percentage of defense contracts are Carve-outs?

Response: No. Not at this time.

Mr. Dunsmore: Are there further questions on the selected topics that you'd like to have the panel address?

Question: There was a reference in one of the earlier talks about sensitive data that is not classified that has to be dealt with. I'm wondering if there's any effort towards dealing with that type of data within classification guides?

Response: The Department of Energy (DOE) has a statutory obligation to protect certain unclassified information as it relates to nuclear weapons. That should be covered in something like that. DoE has a statutory obligation to protect certain unclassified information dealing in the nuclear area, so that would be one. There's no lawful way to withhold information from the public that's not legally classifiable or any other way to protect information. You can't do that. So sensitive information can be withheld from the American public only insofar as the Executive Order, or upper administrative regulations, or the law allows.

Mr. Grau: The Army has looked at this problem.

We do certain things with contractors in this regard. We have had some discussions and correspondence with DIS about the appropriateness of what we do. We are talking to DIS about the subject of unclassified information in the hands of contractors where it would be in the interest of our national defense that it not be disclosed.

As far as your specific question about putting it in classification guidance, we've talked about this as far as the guides themselves are concerned, as differentiated from DD 254s and whether there should be something called an OPSEC annex in guides that are prepared by the Army. I believe all of you would agree that we have enough trouble getting good, logical, effective classification guides prepared without adding this requirement to the guide preparer. However, if we're going to talk OPSEC, and we're going to talk protecting information or giving it some degree of minimal protection, we need to talk about that; and we need to think about that at the same time we decide what is classified and what isn't because the decision processes are very similar and be very related.

Mr. Paseur: In the Air Force, we've also looked at it and elected to not include it in classification guides. Currently we have very active programs in the technology transfer areas aimed at reducing the flow of technology out of the United States. But within the United States and certainly as Mr. Gerald Berkin pointed out, we are walking on thin ice when we start trying to establish requirements for withholding or preventing the release of unclassified types of material within the United States to the American public. We haven't done that.

DIS REGION EVALUATION OF DD FORM 254 ERRORS, PROBLEMS, AND CORRECTIVE SUGGESTIONS

Charles Bell
Classification Management Specialist
Office of Industrial Security
Defense Investigative Service
Atlanta Region

The basic responsibility of the Classification Management (CM) Specialist is to assure that con-

OMISSIONS, ERRORS AND INADEQUATE GUIDANCE ON DD 254 RECEIVED

- **UNDATED**
- **CONTRACTOR NOT IDENTIFIED**
- **LEVEL OF FACILITY CLEARANCE REQUIRED NOT SHOWN**
- **CONTRACT REQUIRES RECEIPT, OR RECEIPT AND GENERATION OF CLASSIFIED MATERIAL WHEN FACILITY HAS NO SAFEGUARDING CAPABILITY**
- **NO GUIDANCE PROVIDED IN BLOCK 15 OF DD 254**
- **NOT SIGNED**
- **SIGNED BY CONTRACTOR PERSONNEL NOT AUTHORIZED, REQUIRES ACO/PCO SIGNATURE**
- **CONFLICTING ACCESS REQUIREMENTS, I.E., 11A ACCESS ONLY, 11B RECEIPT ONLY, 11C RECEIPT AND GENERATION, 11E GRAPHIC ARTS SERVICES ONLY, CHECKED YES**
- **GUIDANCE NOT IN ACCORDANCE WITH EO 12065**
- **GUIDES PROVIDED WITH DD 254 OR REFERENCED NOT REVIEWED (OVER 2 YEARS OLD)**

PROBLEMS IDENTIFIED BY INDUSTRIAL SECURITY REPRESENTATIVE TO CM SPECIALIST FOR RESOLUTION

- CONTRACTOR PERFORMING ON CLASSIFIED CONTRACT, OR SUBCONTRACT — NO GUIDANCE ISSUED
- BIENNIAL REVIEW NOT CONDUCTED
- REQUEST FOR ASSISTANCE ON NON-RESPONSE TO CONTRACTORS
  - REQUEST FOR RETENTION
  - CHALLENGE TO CLASSIFICATION
- REQUEST FOR CLARIFICATION OF GUIDANCE

tractors are provided meaningful classification guidance through all stages of a classified procurement. The fulfillment of this responsibility is dependent on proper notification to the cognizant security office. The method of notification in most cases is the DD Form 254 provided during solicitation stages, at contract award, and subsequently when additions or changes to guidance are desired. In those instances when the cognizant security office is not provided notification of solicitation or award of contract, the end result may well be the compromise of classified information.

In our reviews; we have noted numerous errors in DD Forms 254 from both user agencies and contractors. In fact, there are too many to list or identify individually. Most errors are minor and the action taken is dependent upon the extent of the error, potential impact upon contract performance, and ultimately upon the safeguarding of classified information.

These tables illustrate some of the current errors with the DD Form 254. They are not all inclusive but do reflect those errors which are of a recurring nature. (See Pages 77 & 78)

I would like to discuss some of those errors in more detail.

Omissions. (Total) — As the CM specialist in our region for the past three years, omissions of essentially all blocks on the 254 have been noted. Of all omissions noted, the most common and repetitive are blocks 1, 3, 4, 5, 6, 7, 14, 15 and 16. Blocks 2, 11, 12 and 13 are most always completed. See Page 79)

Omissions (Partial): — Block 6, 10, 12, 14, 15, and 16 are most commonly partially omitted blocks. (See Pages 79 & 80)

Errors (All Blocks) — I do not want to spend too much time on the negative aspects and discussion of errors in each block of the 254. However, I would like to identify the one block which probably causes us most concern. The block in the name, address and zip code of the contractor. The block should reflect the cleared contractor's name and physical location. If classified material is to be released to the contractor facility, it may reflect the mailing address for classified material.

Verification — ISR Para.1-100 — ISM Para. 58

INDUSTRIAL SECURITY REGULATION

"The Cognizant Security Office shall retain their copy of the Facility Clearance Verification for one(1) year after which it shall be destroyed. The recipient of the verification notification shall be immediately notified should a change occur adversely affecting the level of the Facility Clearance or the safeguarding ability of the Facility"

FOR EXERCISE PURPOSES ONLY – SAMPLE DD 254

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION	1. THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO ALL SECURITY ASPECTS OF THIS EFFORT. THE FACILITY CLEARANCE REQUIRED IS: SECRET

2. THIS SPECIFICATION IS FOR:	3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER (Prime contracts must be shown for all subcontracts)	4. DATE TO BE COMPLETED (Estimated)	5. THIS SPECIFICATION IS: (See "NOTE" below. If item b or c is "X'd", also enter date for item a)
a. PRIME CONTRACT	a. PRIME CONTRACT NUMBER		a. ORIGINAL (Complete date in all cases) — DATE
b. SUBCONTRACT (Use item 15 for subcontracting beyond second tier)	b. FIRST TIER SUBCONTRACT NO.		b. REVISED (supersedes all previous specifications) — REVISION NO — DATE
c. REQUEST FOR BID REQUEST FOR PROPOSAL OR REQ FOR QUOTATION	c. IDENTIFICATION NUMBER		c. FINAL — DATE

6 Is this a follow-on contract? [ ] Yes [X] No. If YES, complete the following:

a. _____ (PRECEDING CONTRACT NUMBER) _____ (DATE COMPLETED)

c. Accountability for classified material on preceding contract

Is [ ] Is not [ ] transferred to this follow-on contract.

7a. Name, Address & Zip Code of Prime Contractor *	b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
8a. Name, Address & Zip Code of First Tier Subcontractor *	b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
9a. Name, Address & Zip Code of Second Tier Subcontractor, or facility associated with **IFB, RFP OR RFQ** *	b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office

* When actual performance is at a location other than that specified, identify such other location in Item 15

10a. General identification of the Procurement for which this specification applies	b. DoDAAD Number of Procuring Activity identified in Item 15

c. Are there additional security requirements established in accordance with paragraph 1-114 or 1-115, ISR? [ ] Yes [X] No. If YES, identify the pertinent contractual documents in Item 15

d. Are any elements of this contract outside the inspection responsibility of the cognizant security office? [ ] Yes [X] No If YES, explain in Item 15 and identify specific areas or elements

11. ACCESS REQUIREMENTS	YES	NO	ACCESS REQUIREMENTS (Continued)	YES	NO
a. Access to Classified Information Only at other contractor/Government activities		X	j. Access to SENSITIVE COMPARTMENTED INFORMATION		X
b. Receipt of classified documents or other material for reference only (no generation)		X	k. Access to other Special Access Program information (Specify in Item 15).		X
c. Receipt and generation of classified documents or other material.	X		l. Access to U. S. classified information outside the U. S. Panama Canal Zone, Puerto Rico, U. S. Possessions and Trust Territories.		X
d. Fabrication/Modification/Storage of classified hardware.	X		m. Defense Documentation Center or Defense Information Analysis Center Services may be requested.	X	
e. Graphic arts services only.		X	n. Classified ADP processing will be involved.	X	
f. Access to IPO information.	X		o. REMARKS:		
g. Access to RESTRICTED DATA.	X				
h. Access to classified COMSEC information.	X				
i. Cryptographic Access Authorization required.		X			

12. Refer all questions pertaining to contract security classification specification to the official named below (NORMALLY, thru ACO (Item 16e); EMERGENCY, direct with written record of inquiry and response to ACO) (thru prime contractor for subcontracts).

a. The classification guidance contained in this specification and attachments referenced herein is complete and adequate.

b. Typed name, title and signature of program/project manager or other designated official	c. Activity name, address, Zip Code, telephone number and office symbol

NOTE: Original Specification (Item 5a) is authority for contractors to mark classified information. Revised and Final Specifications (Items 5b and c) are authority for contractors to remark the regraded classified information. Such actions by contractors shall be taken in accordance with the provisions of the Industrial Security Manual.

DD FORM 1 JAN 78 254 EDITION OF 1 APR 71 IS OBSOLETE. ALSO REPLACES DD FORM 254c WHICH IS OBSOLETE

VERIFICATION REQUIREMENTS

INDUSTRIAL SECURITY REGULATION, PARAGRAPH 1-110
(USER AGENCIES)

PRIOR TO DISCLOSURE OF ANY CLASSIFIED INFORMATION TO A FACILITY, THE CONTRACTING ACTIVITY OF THE USER AGENCY SHALL DETERMINE THAT THE CONTRACTOR'S FACILITY HAS A VALID FACILITY SECURITY CLEARANCE EQUAL TO OR HIGHER THAN THE CATEGORY OF CLASSIFIED INFORMATION TO BE DISCLOSED. IF THE FACILITY WILL BE REQUIRED TO HAVE PHYSICAL POSSESSION OF CLASSIFIED MATERIAL, THE CONTRACTING ACTIVITY SHALL ALSO DETERMINE THAT THE FACILITY HAS THE ABILITY TO SAFEGUARD PROPERLY THE CLASSIFIED INFORMATION TO BE DISCLOSED TO OR DEVELOPED BY THE FACILITY.

INDUSTRIAL SECURITY MANUAL, PARAGRAPH 58
(CONTRACTORS)

A. THE PRIME CONTRACTOR SHALL DETERMINE FROM THE COGNIZANT SECURITY OFFICE OF THE PROSPECTIVE SUBCONTRACTOR THAT THE PROSPECTIVE CONTRACTOR HAS BEEN GRANTED AN APPROPRIATE FACILITY CLEARANCE PRIOR TO DISCLOSURE OF ANY CLASSIFIED INFORMATION.

B. PRIME CONTRACTORS, HAVING COMPLIED WITH PARAGRAPH 58A, SHALL DETERMINE THAT PROSPECTIVE SUBCONTRACTORS MEET THE REQUIREMENTS OF THIS MANUAL FOR SAFEGUARDING TOP SECRET, SECRET, AND CONFIDENTIAL MATERIAL PRIOR TO GRANTING POSSESSION OF SUCH MATERIAL TO PROSPECTIVE SUBCONTRACTORS.

When a DD 254 is received by the cognizant security office, one of the first actions taken is verification of facility clearance and safeguarding capability.

INDUSTRIAL SECURITY MANUAL

"Unless otherwise notified in writing by the Cognizant Security Office, each verification furnished in accordance with the paragraph shall remain valid for a period of one calendar year from the date of issuance."

Although normally, notiification is provided to the issuing agency or contractor when the facility name and/or address does not reflect the facility's name and address as maintained by the COG office, we are concerned that classified material may have already been sent to the contractor facility using the erroneous name and/or address which appears on the 254. Of course the result can range from a security violation to compromise of the classified information.

Although the ISR and the ISM do authorized the "Agency" or the "Prime Contractor" to determine the facility clearance and safeguarding capability based on a current contractual relationship involving classified material of the same or higher category as that to be released or developed under the new contract or subcontract, ***we highly recommend (annual) verfication of the performing facility's clearance and safeguarding capability as an additional security assurance.***

DO YOU KNOW WHERE YOUR COGNIZANT SECURITY OFFICE IS?

DEFENSE INVESTIGATIVE SERVICE
DIRECTOR OF INDUSTRIAL SECURITY
805 WALKER STREET
MARIETTA, GA 30060

GEOGRAPHICAL OPERATIONS AREAS

ALL OF:	Alabama
	Florida
	Georgia
	Mississippi
	North Carolina
	South Carolina
	Tennessee
AND PART OF:	Arkansas (47 Counties)
	Louisiana (14 Parishes)
	Missouri (2 Counties)
AND:	Puerto Rico, U.S. Possessions in the Atlantic and Caribbean Area

OTHER COGNIZANT SECURITY OFFICES

Boston, MA	Philadelphia, PA
Cleveland, OH	San Francisco, CA
Dallas, TX	St. Louis, MO
Los Angeles, CA	Washington, D.C.

I would like to clarify that the Cognizant Security Office in all regions are colocated with the DIS Regional Headquarters (HQ) with the following exceptions:

1. The regional DIS HQ for our Cognizant Security Offices is New Orleans.

2. The regional DIS HQ for Cleveland cog nizant security office is Chicago.

3. The regional DIS HQ for St. Louis, MO is Kansas City.

4. The regional DIS HQ for Dallas is San Antonio.

Many DD Form 254s are issued to contractors which reflect erroneous Cognizant Security Offices and certainly do reflect a lack of current information on the part of the issuing activity. Normally, an erroneous name and location of the COG Office results on our (DIS) not knowing that a classified contract has been issued to a contractor until we conduct an inspection of the facility.

We as a service organization are responsible to assure that classified material released to industry is properly safeguarded. However, proper notification must be approved by the COG Office so we are aware of the extent of protection required by the contract.

11 Access Requirements

This is probably one of the most misunderstood portions of the DD Form 254. (See Page 82)

Many 254s are still received which reflect conflicting access requirements.

The access requirements reflected on the 254 are applicable to the premises (contractor facility) to which it is being issued or facility where actual performance will occur. Normally this pertains to a multiple facility environment when the contract is written to the home office but performance is by one of the cleared facilities of the organization.

Access requirements in Block 11 dictate the classification guidance to be approved in Blocks 14 and 15.

A lack of understanding by the contracting agency of the access requirements necessary, may well result in inadequate, misunderstood and confusing guidance. The following example comes to mind of a recent review of a 254. The access requirements reflected "yes" in 11b (receipt of classified documents or other material for reference only, no generation), but Block 15 stated "material generated will be marked in accordance

11. ACCESS REQUIREMENTS	YES	NO
a. Access to Classified Information Only at other contractor/Government activities.		X
b. Receipt of classified documents or other material for reference only *(no generation)*		X
c. Receipt and generation of classified documents or other material.	X	
d. Fabrication/Modification/Storage of classified hardware.	X	
e. Graphic arts services only.		X
f. Access to IPO information.	X	
g. Access to RESTRICTED DATA.	X	
h. Access to classified COMSEC information.	X	
i. Cryptographic Access Authorization required.		X
j. Access to SENSITIVE COMPARTMENTED INFORMATION.		X
k. Access to other Special Access Program information *(Specify in item 15)*.		X
l. Access to U. S. classified information outside the U. S. Panama Canal Zone, Puerto Rico, U. S. Possessions and Trust Territories.		X
m. Defense Documentation Center or Defense information Analysis Center Services may be requested.	X	
n. Classified ADP processing will be involved.	X	
o. REMARKS:		

13a. Information pertaining to classified contracts or projects, even though such information is considered unclassified, shall not be released for public dissemination except as provided by the Industrial Security Manual *(paragraph 5o and Appendix IX)*.

b. Proposed public releases shall be submitted for approval prior to release [ ] Direct [X] Through *(Specify)*:

to the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense *(Public Affairs)* * for review in accordance with paragraph 5o of the Industrial Security Manual.

* *In the case of non-DoD User Agencies, see footnote, paragraph 5o, Industrial Security Manual.*

14. Security Classification Specifications for this solicitation/contract are identified below *("X" applicable box(es) and supply attachments as required)*. Any narrative or classification guide(s) furnished shall be annotated or have information appended to clearly and precisely identify each element of information which requires a classification. When a classification guide is utilized, that portion of the guide(s) pertaining to the specific contractual effort may be extracted and furnished the contractor. When a total guide(s) is utilized, each individual portion of the guide(s) which pertains to the contractual effort shall be clearly identified in Item 14b. The following information must be provided for each item of classified information identified in an extract or guide:
(I) Category of classification. (II) Date or event for declassification or review for declassification, and (III) The date or event for downgrading *(If applicable)*.

The official named in Item 12b, is responsible for furnishing the contractor copies of all guides and changes thereto that are made a part of this specification. Classified information may be attached or furnished under separate cover.

a. A completed narrative is (1) [ ] attached, or (2) [ ] transmitted under separate cover and made a part of this specification.

X b. The following classification guide(s) is made a part of this specification and is (1) [ ] attached, or (2) [X] transmitted under separate cover. *(List guides under Item 15 or in an attachment by title, reference number and date).*

c. Service-type contract/subcontract. *(Specify instructions in accordance with ISR/ISM, as appropriate.).*

d. "X" only if this is a final specification and Item 6 is a "NO" answer. In response to the contractor's request dated _____, retention of the identified classified material is authorized for a period of _____

e. Annual review of this DD Form 254 is required. If "X'd", provide date such review is due: _____.

15. Remarks *(Whenever possible, illustrate proper classification, declassification, and if applicable, downgrading instructions).*

16a. *Contract* Security Classification Specifications for Subcontracts issuing from this contract will be approved by the Office named in Item 16e below, or by the prime contractor, as authorized. This Contract Security Classification Specification and attachments referenced herein are approved by the *User Agency* Contracting Officer or his Representative named in Item 16b below

REQUIRED DISTRIBUTION:

[X] Prime Contractor *(Item 7a)*

[X] Cognizant Security Office *(Item 7c)*

[X] Administrative Contracting Office *(Item 16e)*

[X] Quality Assurance Representative

[ ] Subcontractor *(Item 8a)*

[ ] Cognizant Security Office *(Item 8c)*

[X] Program/Project Manager *(Item 12b)*

[X] U. S. Activity Responsible for Overseas Security Administration

ADDITIONAL DISTRIBUTION:

[ ]

[ ]

[ ]

b. Typed name and title of approving official

c. Signature

d. Approving official's activity address and Zip Code

e. Name, address and Zip Code of Administrative Contracting Office

with source material". What has the contracting officer authorized?

If the contract security classifiction specification does not provide the specifics of the security requirements of the contract then problems are sure to ensue. They may be minor, or they may be major. The end result may be added cost to the Government or to the contractor, or both, or mishandling or compromise of classified information

Block 14 & 15

There has been definite improvement in these areas of the DD Form 254. In most instances, classification guides are being provided along with the 254; when the guides themselves are classified, they are being transmitted separately to contractors.

We still receive occasional 254s with omitted information in Block 14 and no information in Block 15. These are returned with a request to provide adequate and appropriate classification guidance to the contractor.(See Page 83)

Normally, Block 15 of the 254 will contain one or more of the following:

A. Identity of classification guides or extracts furnished by the user agency or contractor.

B. Narrative guidance which identifies the specific types of information to be classified and appropriate downgrading and declassification instruction. When classified hardware is a part of the procedure; the narrative guide should identify each item of classified hardware.

C. When security requirements exceed those in the ISM, special instructions and controls for the handling, processing, storing and transmission of classified information and material.

D. When the contract is for certain types of services, appropriate statements as outlined in Section VII of the ISR and Paragraph 60 of the ISM.

The official named in Block 12b on the DD 254, is responsible for furnishing the contractor copies of all guides and changes thereto that are made a part of the specification.

User agencies should endeavor to afford the contractor the opportunity to participate in the preparation of the DD Form 254. Contractors are encouraged to advise and assist in the development of the classification specification. Ideally, this joint effort should result in classification specifications which are complete, appropriate and sufficient to assure the protection of the classified information to be released or produced under the contract. We continue to receive copies of the obsolete editions of the DD 254 which are no longer authorized and therefore should not be used. Our experience is that the agency or contractor who uses the obsolete DD Form 254, obsolete for over 4 years, is also at least that far behind or more in their knowledge of the Defense Industrial Security Program. I believe that action must be taken now to resolve the seemingly endless issuance or erroneous, incomplete, conflicting and meaningless classification guidance currently being issued to contractors in the DD Form 254. We in DIS can continue to identify problems and errors to user agencies involved, but the "real fix" can only be realized with a coordinated and concentrated education and training effort by those agencies responsible. Both industry and Government must recognize that the DD Form 441 Security Agreement is a joint agreement between the contractor and the U.S. Government with each agreeing to fulfill certain responsibilities stipulated in that agreement. Section 1 of the security agreement begins:

(A) The contractor agrees to . . .
and
(B) The government agrees that . . .

I leave you with this thought. Are you who represent industry and you who represent Government fulfilling your part of the security agreement? A copy of the security agreement, DD Form 441, is shown here. (Page 85 & 86).

DEPARTMENT OF DEFENSE

SECURITY AGREEMENT

THIS AGREEMENT, entered into this day of 19

by and between THE UNITED STATES OF AMERICA through the ~~Defense Contract Administration Services, Defense Supply Agency~~ Defense Investigative Service*

acting for the Department of Defense (*hereinafter called the Government*) and (i)

a corporation organized and existing under the laws of the State of

(ii) a partnership consisting of

(iii) an individual trading as

with its principal office and place of business at in the city of

State of (*hereinafter called the Contractor*).

WITNESSETH THAT:

WHEREAS, the Government, through the Department of the Army, the Department of the Navy, and/or the Department of the Air Force, has in the past purchased or may in the future purchase from the Contractor supplies or services which are required and necessary to the national defense of the United States; or may invite bids or request quotations on proposed contracts for the purchase of supplies or services which are required and necessary to the national defense of the United States; and

WHEREAS, it is essential that certain security measures be taken by the Contractor prior to and after his being accorded access to classified information, and

WHEREAS, the parties desire to define and set forth the precautions and specific safeguards to be taken by the Contractor and the Government in order to preserve and maintain the security of the United States through the prevention of improper disclosure of classified information derived from matters affecting the national defense, sabotage; or any other act detrimental to the security of the United States:

NOW, THEREFORE, in consideration of the foregoing and of the mutual promises herein contained, the parties hereto agree as follows

Section I—SECURITY CONTROLS

(A) The Contractor agrees to provide and maintain a system of security controls within its or his own organization in accordance with the requirements of the Department of Defense Industrial Security Manual for Safeguarding Classified Information attached hereto and made a part of this agreement, subject, however, (i) to any revisions of the Manual required by the demands of national security as determined by the Government, notice of which has been furnished to the Contractor, and (ii) to mutual agreements entered into by the parties in order to adapt the Manual to the Contractor's business and necessary procedures thereunder. In order to place in effect such security controls, the Contractor further agrees to prepare *Standard Practice Procedures* for its or his own use such procedures to be consistent with the Department of Defense Industrial Security Manual for Safeguarding Classified Information. In the event of any inconsistency between the Contractor's Standard Practice Procedures and the Department of Defense Industrial Security Manual for Safeguarding Classified Information as the same may be revised the Manual shall control

(B) The Government agrees that it shall indicate when necessary by security classification (*Top Secret*, *Secret*, or *Confidential*), the degree of importance to the national defense of information pertaining to supplies, services, and other matters to be furnished by the Contractor to the Government or the Government to the Contractor, and the Government shall give written notice of such security classification to the Contractor and of any subsequent changes thereof; provided, however, that matters requiring security classification will be assigned the least restrictive security classification consistent with proper safeguarding of the matter concerned, since overclassification causes unnecessary operational delays and depreciates the importance of correctly classified matter. Further, the Government agrees that when Atomic Energy information is involved it will when necessary indicate by a marking additional to the classification marking that the information is "Restricted Data—Atomic Energy Act, 1946." The Contractor is authorized to rely on any letter or other written instrument signed by the contracting officer changing the classification of matter. The Government also agrees upon written application of the Contractor to designate employees of the Contractor who may have access to information classified Top Secret or Secret or to information classified Confidential when "Restricted Data" is involved, or to matter involving research, development, or production of cryptographic equipment, regardless of its military classification; and alien employees to have access to any classified matter.

(C) The Contractor agrees that it or he shall determine that any subcontractor, subbidder, individual, or organization proposed by it or him for the furnishing of supplies or services which will involve access to classified information in its or his custody has executed a Department of Defense Security Agreement which is still in effect, with any Military Department, prior to being accorded access to such classified information.

Section II—INSPECTION

Designated representatives of the Government responsible for inspection pertaining to industrial plant security shall have the right to inspect at reasonable intervals the procedures, methods, and facilities utilized by the Contractor in complying with the requirements of the terms and conditions of the Department of Defense Industrial Security Manual for Safeguarding Classified Information. Should the Government, through its authorized representative, determine that the Contractor's security methods, procedures, or facilities do not comply with such requirements, it shall submit a written report to the Contractor advising him of the deficiencies

DD FORM 1 OCT 64 441 EDITION OF 1 MAY 54 MAY BE USED

* Pen and ink changes authorized by OSD pending approval of revised form.

Section III—MODIFICATION

Modification of this security agreement (*as distinguished from the Industrial Security Manual for Safeguarding Classified Information, which may be modified in accordance with section I of this agreement*) may be made only by written agreement of the parties hereto.

Section IV—TERMINATION

This agreement shall remain in effect until terminated through the giving of 30 days' written notice to the other party of intention to terminate; provided, however, notwithstanding any such termination, the terms and conditions of this agreement shall continue in effect so long as the Contractor has classified information in his possession or under his control.

Section V—PRIOR SECURITY AGREEMENTS

As of the date hereof, this security agreement replaces and supersedes any and all prior security or secrecy agreements, understandings, and representations with respect to the subject matter included herein, entered into between the Contractor and the Department of the Army, the Department of the Navy, and/or the Department of the Air Force: *Provided*, That the term "security or secrecy agreements, understandings, and representations" shall not include agreements, understandings, and representations contained in contracts for the furnishing of supplies or services to the Government heretofore entered into between the Contractor and the Department of the Army, the Department of the Navy, and/or the Department of the Air Force.

Section VI—SECURITY COSTS

This agreement does not obligate Government funds, and the Government shall not be liable for any costs or claims of the Contractor arising out of this agreement or instructions issued hereunder. It is recognized, however, that the parties may provide in other written contracts for security costs which may be properly chargeable thereto.

IN WITNESS WHEREOF, the parties hereto have executed this agreement as of the day and year first above written:

THE UNITED STATES OF AMERICA

By _____

_____
(Authorized representative of the Government)

_____
(Corporation)

WITNESS

By _____

_____ _____

_____
(Firm)

_____
(Title)

_____
(Address)

NOTE.—In case of corporation, witnesses not required but certificate below must be completed. Type or print names under all signatures.

NOTE.—Contractor, if a corporation, should cause the following certificate to be executed under its corporate seal, provided that the same officer shall not execute both the agreement and the certificate.

CERTIFICATE

I, _____, certify that I am the _____ of the corporation named as Contractor herein; that _____ who signed this agreement on behalf of the Contractor, was then _____ of said corporation; that said agreement was duly signed for and in behalf of said corporation by authority of its governing body, and is within the scope of its corporate powers.

(*Corporate Seal*)

_____
(Signature)

GPO 886-110

FACILITY SECURITY INSPECTION SKIT "COULD BE YOURS" FACILITY

Eugene (Gene) J. Suto
Director of Security
General Research Corporation
McLean, Virginia

The idea for the original script for the debrief "Could Be Yours" Facility was conceived in early 1981. At that time it was felt a different approach was needed to put on a training-education program of security inspection problems for the NCMS Washington, D.C. Chapter Mini-Seminar to be held during April 1981 at the Naval Surface Weapons Center.

The skit was so well received that when Huntsville, Alabama, decided to put on a NCMS Mini-Seminar in November 1981, they also wanted to use the script. The group, therefore, was named the "NCMS Players." Several of the Players have turned in such outstanding performances that they are almost known by the parts they play, such as Sandy Waller who has performed as Miss Woo Woo, Elmer Hargis as Mr. Do Wrong, Cheryl Cross as Miss Lamebrain, and Pam Hart as Miss Stampit. All performers have done well indeed. The script has been rewritten and expanded somewhat for the NCMS National Seminar at Orlando, Florida.

After the session, our Players will pass out to you a personal as well as company "Security Inspection Sheet" on which you may want to rate yourself and your company as to your security habits. In this skit we plan to highlight common security mistakes at facilities. In doing so, we hope you take home ideas on how to improve your own programs. Although normally employees of a facility are not part of a debrief, they have been added in this case to highlight these problem areas.

During this session we plan to take you through a debrief meeting of the "Could Be Yours" facility. To set the stage, Government Inspectors have been on the premises of the "Could Be Yours" Facility going over records about the Information Security Program of the U.S. Government.

The inspection has now been completed and a debrief session is to take place. This inspection is geared toward a Government contractor but data presented can be slanted toward Government as well. To play the various roles, during the past year, we formed the NCMS Players. This is a truly professional group and some may even be nominated for Oscars. The people have been acting in real life for years but only now can we witness their true talents. Now, on with the show!

Playing the part of Mr. Regulation - Government Security Supervisor is:
Mr. Fred Badin
Security Administrator
IBM Corporation
Gaithersburg, Maryland

Ms. Catchall - Government Security Inspector is:
Ms. Liz Heinbuch
Security Manager
Office Deputy Chief of Staff for R.D.A.
Department of the Army
Washington, D.C.

Mr. Watchit - Contractor Security Director is:
Mr. Jim Bagley
President
RB Associates
Falls Church, Virginia

Mr. Howcome - Contractor Management Official is:
Mr. Ron Munday
Chief, Facilities Division
Defense Investigative Service
Norcross, California

Mr. Do Wrong - Contractor Engineer/Scientist is:
Mr. Elmer Hargis
Security Officer
Ballistics Missile Defense Command
Huntsville, Alabama

Ms. Lamebrain - Contractor Engineer/Scientist is:
Ms. Cheryl Cross
Security Specialist
Naval Surface Weapons Center
Silver Spring, Maryland

Ms. Stampit - Contractor Document Clerk is:
Ms. Pamela Hart

Vice President
ALM Inc.
Arlington, Virginia

And, Ms. Woo Woo - Contractor Secretary is:
Ms. Sandy Waller
Industrial Security Specialist
Defense Investigative Service
Washington, D.C.

Mr. Regulation:
Mr. Howcome, Mrs. Catchall, and I have just completed a three day inspection of your facility and are indeed sorry to say we have found some disturbing and serious deficiencies and violations in your facility. I will discuss each of these deficiencies and my Inspector, Ms. Catchall, will assist me. These are items that will be placed in a letter to the president of your facility. You will have an opportunity to respond in writing within thirty days. First of all, i wish to advise you, your classified container combinations are not being properly protected. In two cases combinations were not being properly safeguarded.

Mr. Howcome:
What do you mean? This same thing happened during our last inspection and I thought everyone was properly indoctrinated.

Mr. Watchit:
Chief, let me explain. In one case Ms. Woo Woo here produced a combination and her actions embarrassed me. - but I retrieved the combination and burned it.

Ms. Woo Woo:
I had the combination in a safeplace — here, let me show you. I pulled it out from my bra — not even by boyfriend can get at it! I didn't realize this was a violation. I won't do it again.

Mr. Howcome:
You did what? I'll see you later in private, Ms. Woo Woo. Did you change the combination, Mr. Watchit? Who was the other violator?

Mr. Watchit:
Yes, Chief, I changed the combination. The other person was Mr. Do Wrong. He had his combination written on his blackboard.

Mr. Howcome:
He did what? Didn't he know better?

Mr. Do Wrong:
Please let me explain. Ms. Lamebrain and I share a safe. I was leaving for the day and she called me and said she forgot the number. I told her I would write it on the blackboard with a mathematical formula — then only she and I would know it. I saw nothing wrong in this — but somehow Ms. Catchall caught it and opened my safe!

Mr. Watchit:
Chief, Mr. Do Wrong has again been re-indoctrinated. I also changed his safe combination. He as well as his entire group have been told again they cannot write down combinations anywhere.

Mr. Howcome:
I'll deal with you later, Do Wrong. I'm surprised at your actions.

Mr. Regulation:
You realize there could have been a serious compromise in each of these cases?

Mr. Howcome:
I hope there wasn't anything else serious like this.:

Mr. Regulation:
Well Sir, there is another violation. As a matter of fact as we were performing the inspection, a safe was left open and unattended.

Mr. Watchit:
Chief, this happened again in Mr. Do Wrong's office. It's really not as bad as it sounds. Let Mr. Do Wrong explain.

Mr. Howcome:
Well, Do Wrong, would you explain? You seem to be causing all our problems.

Mr. Do Wrong:
Yes Sir. I meant no harm, but you see, Sir, I had a bad case of diarrhea yesterday. I had all my classified papers out on my desk and all of a sudden I had to go. Well, I grabbed everything I could and threw it in the safe and spun the dial quickly and ran. I was back in two minutes and there was this Inspector and our Security Director standing at my

safe - which was open. I don't see how they did it -because I closed it.

Ms. Catchall:
Sir, a safe is not closed unless the dial is spun at least four times in any direction and each drawer checked. I just turned the combination back to zero and opened it - just like that. Furthermore, there was no one in attendance in the area. How do I know Mr. Do Wrong was gone only two minutes.

Mr. Watchit:
Chief, Mr. Do Wrong did come running back, tucking in his shirt in his pants. I presume what he said is true. Nevertheless I am re-indoctrinating him on proper procedures.

Mr. Howcome:
Do Wrong, this isn't your day - I hope you have learned your lesson. You can expect a Letter of Reprimand.

Mr. Regulation:
Let me discuss our next serious problem. During the inspection we found several documents in *safes that had not been placed into the facility* accountability system. As you are aware, all classified documents, regardless of classification, must be entered into your accountability system.

Mr. Watchit:
Sir, Mr. Do Wrong had a Confidential document in his safe and it was laying right on top of all his other materials. Mr. Do Wrong and Ms. Woo Woo have access to the safe.

Ms. Woo Woo:
I don't know how it got there, because a few days before the inspection I checked everything in the safe and I didn't see that document. In fact, Mr. Do Wrong came back later to the office to see me.

Ms. Catchall:
Sir, first, let me clarify. It could be referred to as a document but it was actually a two page letter and only one paragraph was Confidential.

Mr. Howcome:
Do Wrong, how did you get that letter?

Mr. Do Wrong:
Sir, I was at the Pentagon visiting our customer, Colonel Follow Me. Colonel Follow Me said, "Here take this. It will help clarify your project." I have always taken secret and confidential documents Colonel Follow Me gave me — without questions and brought them back to the facility.

Ms. Catchall:
Ah ha — did you sign a receipt? There could be another violation here.

Mr. Watchit:
Wait a minute — you know a receipt isn't necessary for a confidential document, and in this case only one paragraph of the letter was classified.

Mr. Do Wrong:
Since I came back to the plant late — to pick up Ms. Woo Woo — I threw the letter in the safe, I simply forgot to get it to the document office the next morning to place it in the accountability system. In fact the front of the letter was poorly marked.

Mr. Watchit:
Well sir, we did retrieve the letter and have it properly in the control system now. It has all the proper markings. To my knowledge there was no secret information involved.

Mr. Howcome:
What were the other documents not in the system?

Mr. Watchit:
Sir, Ms. Lamebrain also had a secret document marked "Pentagon Working Paper — Eyes Only —Sensitive."

Mr. Howcome:
Is Lamebrain here?

Ms. Lamebrain:
Here I am, sir.

Mr. Howcome:
Ms. Lamebrain, how did you get that document and why wasn't it in our accountable system?

Ms. Lamebrain::
Sir, Colonel Big Wheel was here last week on a visit and brought the document with him. He had no intention of leaving it here, but the meeting he attended lasted until quitting time. We had a cocktail party afterward and Colonel Big Wheel met Ms.

Woo Woo. It didn't look like he would get back to the Pentagon. He asked if I could place the document in my safe for him until the next morning. I agreed. He failed to come by the next day, however, and we both forgot about it until the inspector checked the safe and there it was. It's not our document — I shouldn't be blamed for its presence.

Ms. Woo Woo:
We really had a blast! Big Wheel is SOME BIG WHEEL!

Mr. Watchit:
Sir, we could have placed the document in our control system and returned it by courier to Colonel Big Wheel. That would have been the prudent thing to do.

Mr. Howcome:
Ms. Lamebrain, see Mr. Watchit after our meeting on how to handle these matters in the future.

Mr. Regulation:
Sir, in talking to Ms. Stampit, we discovered another case of improper transmittal and handling of secret information.

Mr. Howcome:
What do you mean?

Mr. Regulation:
Ms. Stampit indicated to us that recently while she was at the Pentagon she was asked to bring a secret document back to the facility.

Mr. Stampit:
I saw nothing wrong with what I did. My sponsor handed me this secret document and I placed the document in my briefcase.

Mr. Regulation:
Ms. Stampit you did NOT double wrap the document!

Ms. Stampit:
In transmitting the document it was in my briefcase and in my car. Isn't that double wrapping?

Mr. Regulation:
A very technical definition of double wrapping but still NOT considered double wrapped in accordance with Government regulations.

Mr. Howcome:
Ms. Stampit I'm surprised at you. I thought you were up on these procedures. You need further indoctrination on wrapping of documents. Mr. Watchit see what you can do later with Ms. Stampit.

Mr. Watchit:
Right Chief, I will talk to here and show her how to properly wrap classified documents. I did state in my instructions to the staff that placing items in a briefcase was not a proper method of wrapping.

Mr. Regulation:
Sir, a number of your staff including Ms. Lamebrain are not using portion marking properly.

Mr. Howcome:
What do you mean by portion marking?

Mr. Regulation:
Well it was similar to paragraph marking except with portions you should be able to point anywhere to an item in a document and know its classification. We found on a number of photos in a classified document that the classification was not properly indicated.

Mr. Watchit:
Chief, I put out a memo about portion marking a long time ago.

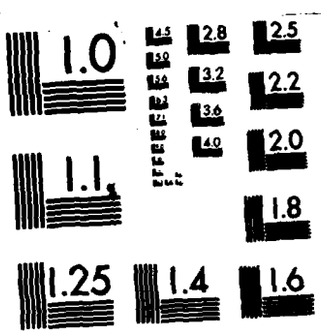
Mr. Regulation:
Do you know that the Dept. of Defense has a contractor's booklet on marking? This would be of great assistance to you and your staff.

Mr. Watchit:
I gave a copy of this booklet to Ms. Lamebrain.

Mr. Howcome:
Lamebrain, where are you? Do you still have the copy?

Ms. Laimbrain:
I'm here, Sir. I filed the booklet in file 13, but I can't remember where file 13 is now!

Mr. Howcome:
Don't you know file 13 is the wastebasket. See if Mr. Watchit can get you another copy.



Ms. Lamebrain:
I'll try to hold onto the next copy, Sir.

Mr. Regulation:
Our next item is one of a serious nature with respect to classification. Several of your staff had classified reports and had failed to place the proper classification authority on such reports.

Mr. Watchit:
Sir, in one of these cases Ms. Lamebrain was at fault — let her explain.

Ms. Lamebrain:
I'm really sorry about this, but I thought I was doing the right thing. I was writing this report on a meeting I had attended and wasn't really sure if the information was classified or not and had forgotten the source data. Well, I pulled out my good luck coin like this — and said "heads it's secret, tails it's unclassified." Heads it was, so I marked it classified by me.

Mr. Watchit:
It was a case of improper security classification guidance. We will have the matter corrected.

Mr. Howcome:
Ms. Lamebrain, don't you know any other way of classification?

Ms. Lamebrain:
Yes Sir, I do. I have often used the dartboard in our conference room. I quit using that though, since I missed the dartboard last time and the dart his Ms. Woo Woo. She hasn't been able to sit down since!

Mr. Howcome:
Watchit, don't we get proper security classification guidance on our contracts?

Mr. Watchit:
We got a DD 254 "Security Contract Classification Form" on Ms. Lamebrain's contract but no classification guide was enclosed with it. I had queried our contracting officer for additional guidance, but to date have not received it. Ms. Lamebrain should have come to me and I would have followed up on getting proper guidance.

Mr. Regulation:
Sir, we also found a case of improper transmittal of British RESTRICTED material and further that material was not properly marked and entered into your accountability system.

Mr. Howcome:
How did that happen? Is RESTRICTED a classification? I thought we got rid of that years ago.

Mr. Watchit:
Yes, the U.S. did, but the NATO countries still carry the marking. One of our staff went on a visit to the U.K. and he explained that he was given a briefing which he was told was unclassified. He asked that the information be sent to him and it was sent by First Class mail to his office. There was a typewritten marking at the top of the briefing — RESTRICTED. He thought he was doing the right thing by placing it in his safe. He forgot to bring it to document control and to have it marked "Handle as U.S. CONFIDENTIAL."

Mr. Howcome:
I'm afraid, Sir, the regulation indicates an improper transmittal and then a failure by the contractor to mark it properly. Now, if the U.K. had sent it to the U.S. Government and the U.S. Government representative handed it to your employee, it would have been OK. I know our U.S. representatives would always carefully mark it "Handle as a U.S. CONFIDENTIAL." That is what should have happened in this case.

Mr. Howcome:
Watchit, be sure you provide guidance in your indoctrinations to avoid future problems like this.

Mr. Watchit:
Yes Sir, I will.

Mr. Regulation:
Our next item is a situation of improper transmittal and storage of classified material. Two of your employees took a trip and kept classified material overnight in their hotel room.

Mr. Watchit:
Yes Mr. Howcome, I have identified them. Ms. Stampit and Mr. Always-Late were attending a conference on the west coast, and they were asked to come by the security office to be designated couriers and receive instructions, but they bypassed our office.

Ms. Stampit:
Mr. Always-Late didn't finish his vugraph briefing on time and I stayed late to help him. We had to by-pass security if we were to make our flight at McCoy at the end of the day. Well, our plane was delayed and the airlines wanted to treat us right, so everyone was given free drinks. Mr. Always-Late and I reached L.A. about 1:00 a.m. and was he ever smashed! I admit I wasn't feeling any pain either! Well, we went first to the hotel room to drop off our luggage and planned to go and drop off the classified vugraphs at the facility. Well, Mr. Always-Late passed out in my room. I couldn't leave him, so I stayed there all night with the material under my mattress. Boy, was I bushed! What a trip! The material was not compromised. I know I certainly was not! We finally got to the facility at 8 a.m.

Ms. Catchall:
They should have gone directly to the facility and stored the materials properly regardless of the hour.

Ms. Stampit:
Yes, I realize that now.

Mr. Howcome:
Ms. Stampit I'll deal with you and Always-Late later!

Mr. Regulation:
Your employees have been using word processors for classified processing without advance security approval.

Mr. Watchit:
The director of the production department said there were no plans to use the word processor for classified work. Then I found Ms. Stampit operating it on classified work.

Ms. Stampit:
I don't see anything wrong. It's just like a typewriter and I don't need security approval to use my electric typewriter. I did mark my ribbon and when the ribbon wasn't used I put in in my desk.

Ms. Catchall:
Don't you realize that regulations require our office to approve your security procedure before you use the word processor — just like a computer. Further, you should have stored the ribbon in a safe.

Ms. Stampit:
That's silly. It's really not a computer. Why do I have to follow such a requirement?

Mr. Watchit:
This is a new requirement, and we are doing our best to follow it. I am getting our employees briefed but some still don't see the reason for such complex procedures.

Mr. Howcome:
Mr. Watchit, be sure they follow the procedure as we should live with the new requirements..

Mr. Watchit:
Yes Sir.

Mr. Regulation:
We have informed your security director, Mr. Watchit, that not withstanding any previous approvals by our office, an evaluation of strongrooms currently in use by your facility revealed some areas in question do NOT meet the new construction criteria for strongrooms.

Mr. Howcome:
Watchit, I thought we were in good shape on strongrooms. As I recall this matter has not come up for many years. Why raise the problem now?

Mr. Watchit:
Sir, everytime we have been inspected in the last several inspections, each inspector has come up with his own interpretation of the regulations. When we first built these strongrooms we asked if alarms could compensate for bars on windows and similar safeguards and the answer was "yes." No one would ever give us this in writing, however, and since we always passed inspection, we felt we were OK. We had spent the money on alarms. Now we are being asked to correct so-called deficiencies that currently exist because standards are being changed. The current inspectors do not want to accept what past inspectors approved. It really comes down to new standards, Sir, and we may have to spend a considerable amount of money. I really don't see eye to eye with the Government on this issue and feel we should refer it to their higher headquarters for resolution.

Mr. Regulation:
You do have the option of going to our higher headquarters thru channels.

Mr. Howcome:
That we will do in this case. Perhaps President Reagan will remove this new regulation and requirement as unnecessary and overly costly.

Mr. Regulation:
We aren't thru yet. We still have a few items. Ms. Catchall and I have found that you have several Top Secret cleared persons who have not used their clearances for over 18 months.

Ms. Catchall:
Yes, it costs the Government money to clear these people and they should not be cleared for T/S if their work will not require it.

Mr. Watchit:
Sir, Ms. Woo Woo has stated she has not used her Top Secret clearance.

Ms. Woo Woo:
I haven't seen a Top Secret document since I have been here and that is two years now. Do I have to lose my clearance?

Mr. Howcome:
We do have a need for Ms. Woo Woo's skills — I mean typing skills and we should hold on to her Top Secret clearance. Watchit, see what you can do for us.

Mr. Watchit:
Yes Sir.

Mr. Howcome:
Mr. Regulation, didn't you find any good points during your inspection of our facility?

Mr. Regulation:
Yes, I did. For one thing, you have a very attractive receptionist who greeted us as we entered your facility. She certainly had some good points.

Mr. Howcome:
I didn't mean that kind of point. I meant don't we have some good security procedures in effect. How indoctrinated were other members of our staff on security matters?

Mr. Regulation:
Well, for one your security awareness program seems to be working well. Your security staff has sent out several good awareness bulletins in the past few months. I believe Ms. Woo Woo has one she showed us that will impress you.

Ms. Woo Woo: (unfolding and rolling out paper towel)

Here's an awareness bulletin that made all employees sit down and take notice. The security department told us all about the interception of communications in this one. It starts out — Al Hello Al. You're flying right over me. Can you here me?

Ms. Catchall:
That's a fine security brief. Boy, if the Soviets intercept the President out over the ocean you know your company could be a sitting duck right next to Embassy Row in Washington.

Mr. Howcome:
That's great. What else do you have to report?

Ms. Woo Woo:
Well, Sir, I reported to Security Information about two Russian Agents who were asking me about certain reports our firm had published. I asked them for their complete I.D.'s. Believe me, I did, and they showed me. The reports they wanted were unclassified, but they had not been released to the press. They didn't get anything from me —no Sir!

Mr. Watchit:
She sure did, Chief, and I made a proper report to the FBI and other Government authorities.

Mr. Regulation:
Sir, we also found you had a good visitor clearance program in effect. Most of your visitor clearances were processed in time and no one was left stranded at any facility except for one trip made by Mr. Do Wrong to NATO.

Mr. Howcome:
What happened again to Do Wrong?

Mr. Watchit:
Well, Sir, Do Wrong just didn't give us any advance notice and took off to NATO. We should have about 30 days notice to clear his trip with all the authorities.

Mr. Howcome:
Do Wrong, where are you? Why can't you give security more time?

Mr. Watchit:
Do Wrong told me he had enough problems getting tickets and a passport much less worrying about security! He said, "Let security worry about me." Normally when he goes on a trip, most people know him and let him in, but this time he was stopped.

Mr. Regulation:
Yes, a report came to us through channels that he was not admitted to the NATO faciities he wanted to visit.

Mr. Howcome:
I just don't know about Do Wrong. We will examine his case in detail.

Mr. Regulation:
Ms. Catchall and I found several other minor items wrong. Such as stamping and marking work papers and other documents, but these were corrected on the spot. We will not include such minor items in our report. We will, however, return to our office and write up our findings which your president should receive in a few days, after which you will have 30 days to respond. We wish to thank Mr. Watchit and his staff for their cooperation. They appear to be doing a good job under trying circumstances. It appears they need more management support. For your information, a new Executive Order on security classification has been issued and you should be aware there will be some changes. Wait for proper instructions.

Mr. Howcome:
It appears as though we have some buttoning up to do in our facility. We must also start a security education program to properly indoctrinate personnel in all their responsibilities. There are a few items you have mentioned that require further clarification and resolution, such as our use of word processors, and the new requirements for strongrooms. I assure you that we wish to strengthen our security program and I am directing Mr. Watchit to work closely with you.

Moderator:
(Gene Suto)
Well, there you have it Ladies and Gentlemen, problems in the "Could be Yours" Facility. Let me summarize some of the problem areas:

1. Combinations - know how to handle them.
2. Safes being left open, unattended or improperly closed.
3. Documents not being placed in the accountability system.
4. Improper classification and markings.
5. Improper transmission.
6. Improper actions on trips and not storing documents properly.
7. New problems — word processors.
8. Strongroom requirements.
9. Clearance problems.

These are just selected areas, but they point up to one thing — SECURITY EDUCATION. How do you rate? Well, our NCMS Players will hand out to you a Security Inspection Check Sheet. Thank you for your attention. We are here to answer questions as they may arise(Inspection Sheet Pages 95-97)

COMPUTER/WORD PROCESSING SECURITY: HOW TO OBTAIN SYSTEM APPROVAL AND MAINTAIN EFFECTIVE SECURITY

Richard F. Williams, CPP
Chief, Industrial Security Program Division
Defense Investigative Service, DoD

Section XIII of the Industrial Security Manual (ISM) establishes security measures for the safeguarding of classified information contained in or processed by ADP systems and word processors in the custody and control of contractors in the

(Continued on Page 98)

SECURITY OFFICE INSPECTION CHECK SHEET
INDIVIDUALS

GOVERNMENT SECURITY REGULATIONS REQUIRE A CONTRACTOR TO REVIEW HIS SECURITY SYSTEM ON A CONTINUING BASIS AND TO SCHEDULE SELF-INSPECTIONS MIDWAY BETWEEN THE LAST AND NEXT INSPECTION. TO ASSIST THE FACILITY SECURITY REPRESENTATIVE IN THIS INSPECTION, AND TO ASSURE THAT YOUR RECORDS ARE IN ORDER, IT IS IMPORTANT THAT EACH PERSON PERFORM A SELF-INSPECTION. ASK YOUR SELF THESE QUESTIONS:

		YES	NO
1.	ARE MY CLASSIFIED HOLDINGS AT THE ABSOLUTE WORKING MINIMUM?		
2.	CAN I QUICKLY PRODUCE ALL ACCOUNTABLE CLASSIFIED MATERIAL IN MY POSSESSION FOR INSPECTION?		
3.	ARE ALL CLASSIFIED MATERIALS (INCLUDING WORK PAPERS, DRAFTS AND FINALS) IN MY POSSESSION PROPERLY MARKED?		
4.	HAVE I RETURNED OUTDATED CLASSIFIED WORK PAPERS TO DOCUMENT CONTROL FOR DISPOSITION?		
5.	AM I STORING CLASSIFIED MATERIAL IN PROPER CONTAINERS?		
6.	DO I HAVE A CURRENT INVENTORY OF ALL ACCOUNTABLE DOCUMENTS CHARGED TO ME?		
7.	DO MY VISITORS WHO DISCUSS CLASSIFIED INFORMATION HAVE AN APPROVED "UP-TO-DATE" CLEARANCE AND "NEED-TO-KNOW" ON FILE IN THE SECURITY OFFICE?		
8.	AM I PLACING CLASSIFIED WASTE MATERIAL (WORKING PAPERS, CARBONS, TYPEWRITER RIBBONS, PRINTOUTS, ETC.) IN PROPERLY MARKED BURN BAGS?		
9.	AM I LEAVING CLASSIFIED MATERIAL UNATTENDED AT ANY TIME?		
10.	HAVE I RECORDED MY SAFE COMBINATION IN ANY LOCATION WITHOUT SECURITY APPROVAL?		
11.	DO I COORDINATE WITH THE SECURITY OFFICE IN ARRANGING CLASSIFIED MEETINGS?		
12.	HAVE I REPORTED REQUESTS FOR INFORMATION RECEIVED FROM COMMUNIST SOURCES, WHETHER BY LETTER, TELEPHONE OR PERSONAL CONTACT?		
13.	HAVE I RECEIVED CLASSIFIED INFORMATION FROM ANY SOURCE WHICH HAS NOT BEEN ENTERED INTO THE DOCUMENT CONTROL SYSTEM?		
14.	HAVE I REMOVED CLASSIFIED INFORMATION FROM THE FACILITY WITHOUT OBTAINING THE APPROVAL OF THE SECURITY OFFICER?		
15.	DO I DISCUSS CLASSIFIED INFORMATION IN PUBLIC PLACES OR OVER THE TELEPHONE?		
16.	DO I HANDLE CLASSIFIED MATERIAL PROPERLY WHILE ON A BUSINESS TRIP, STORING IT ONLY AT CLEARED FACILITIES?		
17.	AM I GETTING SECURITY APPROVAL BEFORE I USE COMPUTERS, WORD PROCESSORS OR RELATED EQUIPMENT FOR CLASSIFIED PROCESSING?		
18.	DO I REALLY NEED ALL THE CLEARANCES I CURRENTLY HAVE?		
19.	HAVE I REPORTED ADVERSE INFORMATION ABOUT FELLOW EMPLOYEES TO THE SECURITY OFFICE?		

QUESTIONS 1 TO 8, 11, 12, 16 AND 19 SHOULD HAVE BEEN ANSWERED YES.

QUESTIONS 9, 10, 13, 14 AND 15 DEMAND NO AS THE PROPER ANSWER.

IF YOU HAVE NOT ANSWERED ALL QUESTIONS CORRECTLY, TAKE IMMEDIATE ACTION TO CORRECT ANY DEFICIENCY. SECURITY PERSONNEL ARE READY TO ASSIST YOU IN MAKING YOUR SECURITY HABITS 100 PERCENT EFFECTIVE.

SECURITY OFFICE INSPECTION CHECK SHEET
ORGANIZATIONS

GOVERNMENT SECURITY REGULATIONS REQUIRE A CONTRACTOR TO REVIEW HIS SECURITY SYSTEM ON A CONTINUING BASIS AND TO SCHEDULE SELF-INSPECTIONS MIDWAY BETWEEN THE LAST AND NEXT INSPECTION. HOW DOES YOUR OFFICE RATE?

ANSWER THESE QUESTIONS TRUTHFULLY AND FIND OUT.

		YES	NO	N/A
1.	ARE CLASSIFIED HOLDINGS OF THE STAFF AT THE ABSOLUTE WORKING MINIMUM?			
2.	CAN STAFF MEMBERS QUICKLY PRODUCE ALL ACCOUNTABLE CLASSIFIED MATERIAL IN THEIR POSSESSION FOR INSPECTION?			
3.	ARE ALL CLASSIFIED MATERIALS (INCLUDING WORK PAPERS, DRAFTS AND FINALS) PROPERLY MARKED?			
4.	HAVE OUTDATED CLASSIFIED WORK PAPERS BEEN RETURNED TO DOCUMENT CONTROL FOR DISPOSITION?			
5.	ARE STAFF STORING CLASSIFIED MATERIAL IN PROPER CONTAINERS?			
6.	DOES DOCUMENT CONTROL HAVE CURRENT INVENTORIES OF ACCOUNTABLE DOCUMENTS CHARGED TO STAFF MEMBERS?			
7.	DO VISITORS WHO DISCUSS CLASSIFIED INFORMATION HAVE "UP-TO-DATE" CLEARANCES AND "NEED-TO-KNOW" ON FILE IN THE SECURITY OFFICE?			
8.	IS CLASSIFIED WASTE MATERIAL (WORKING PAPERS, CARBONS, TYPEWRITER RIBBONS, PRINTOUTS, ETC.) TURNED IN FOR PROPER DESTRUCTION?			
9.	IS ANY CLASSIFIED MATERIAL THROUGHOUT THE FACILITY UNATTENDED AT ANY TIME?			
10.	HAS ANY STAFF RECORDED SAFE COMBINATIONS IN ANY LOCATION WITHOUT SECURITY APPROVAL?			
11.	DOES THE STAFF COORDINATE WITH THE SECURITY OFFICE IN ARRANGING CLASSIFIED MEETINGS?			
12.	HAVE STAFF REPORTED REQUESTS FOR INFORMATION RECEIVED FROM COMMUNIST SOURCES, WHETHER BY LETTER, TELEPHONE OR PERSONAL CONTACT?			
13.	DO ANY STAFF RECEIVE CLASSIFIED INFORMATION FROM ANY SOURCE WHICH HAS NOT BEEN ENTERED INTO THE DOCUMENT CONTROL SYSTEM?			
14.	ARE YOU AWARE OF CLASSIFIED INFORMATION REMOVED FROM THE FACILITY WITHOUT OBTAINING SECURITY OFFICE APPROVAL?			
15.	ARE YOU AWARE OF CLASSIFIED INFORMATION DISCUSSED IN PUBLIC PLACES OR OVER THE TELEPHONE?			
16.	ARE YOUR STAFF HANDLING CLASSIFIED MATERIAL PROPERLY WHILE ON A BUSINESS TRIP, STORING IT ONLY AT CLEARED FACILITIES?			
17.	DO YOUR EMPLOYEES GET SECURITY APPROVAL BEFORE USING COMPUTERS, WORD PROCESSORS OR RELATED EQUIPMENT FOR CLASSIFIED PROCESSING?			
18.	IS YOUR OFFICE PROCESSING ANY UNNEEDED CLEARANCES?			
19.	DOES YOUR OFFICE REPORT ADVERSE INFORMATION ABOUT FELLOW EMPLOYEES?			
20.	DOES YOUR FACILITY HAVE A SECURITY EDUCATION PROGRAM IN EFFECT?			
21.	IS YOUR FACILITY PROPERLY PORTION MARKING CLASSIFIED DOCUMENTS?			
22.	DO YOU KEEP REQUISITE CLASSIFICATION GUIDES FOR YOUR FACILITY ON HAND FOR READY REFERENCE?			

SECURITY INSPECTION CHECK SHEET — Continued
ORGANIZATIONS

		YES	NO	N/A
23.	DOES YOUR OFFICE REVIEW ALL DD 254's RECEIVED FOR ACCURACY AND PROPER DISTRIBUTION?			
24.	HAS YOUR OFFICE EVER PARTICIPATED IN THE REWRITE OR CORRECTION OF AN IMPROPER DD 254?			
25.	HAS YOUR OFFICE EVER CHALLENGED THE IMPROPER CLASSIFICATION OR MARKING OF A CLASSIFIED REPORT?			
26.	DOES YOUR OFFICE HAVE AN UP-TO-DATE REVIEW AND RETENTION PROGRAM IN EFFECT?			
27.	DOES ANYONE IN YOUR SECURITY/CLASSIFICATION OFFICE REVIEW PUBLICATIONS FOR PROPER CLASSIFICATION AND MARKINGS BEFORE REPRODUCTION?			
28.	ARE FOREIGN CLASSIFIED DOCUMENTS — SUCH AS NATO RESTRICTED — MARKED WITH PROPER US MARKINGS?			
29.	DOES YOUR OFFICE FOLLOW UP ON OUTSTANDING RECEIPTS?			
30.	IS REPRODUCTION OF CLASSIFIED INFORMATION HELD TO A MINIMUM?			
31.	DOES YOUR OFFICE HAVE AN ONGOING DESTRUCTION PROGRAM FOR UNNEEDED REPORTS?			
32.	DOES YOUR OFFICE KEEP ON HAND UPDATED SECURITY REFERENCES AND REGULATIONS?			
33.	DO PERSONNEL OF YOUR OFFICE KEEP ABREAST OF NEW SECURITY/CLASSIFICATION REQUIREMENTS?			
34.	ARE YOU AND YOUR STAFF AWARE OF THE NATIONAL CLASSIFICATION MANAGEMENT SOCIETY (NCMS) AND MEMBERSHIP BENEFITS?			

QUESTIONS 1 TO 8, 11, 12, 16, 17, 19, AND 20 TO 34 SHOULD HAVE BEEN ANSWERED YES.

QUESTIONS 9, 10, 13, 14, 15 AND 18 DEMAND NO AS THE PROPER ANSWER.

IF YOU HAVE NOT ANSWERED ALL QUESTIONS CORRECTLY YOUR OFFICE NEEDS SOME BUTTONING UP ACTION IN YOUR FACILITY!

Defense Industrial Security Program (DISP). Section XIII specifies conditions and prescribes security requirements under which these systems must be operated when handling classified information. It provides that, in addition to the other requirements of the ISM classified information contained in an ADP system shall be safeguarded by the continuous employment of protective features in the system's hardware and software, as well as by other administrative, physical and personnel security controls and constraints. ADP system security is totality of protective controls and constraints over the following areas:

- Hardware configutation — to provide stability and reliability.
- Software design — to ensure integrity.
- Personnel — to provide for individual accountability.
- Operational procedures — to insure data integrity and information control.
- Physical environment — to minimize unauthorized access.
- Communications — to provide secure lines and links.

Objectives

The objectives of the DIS ADP Security Program is to assure that an ADP system which handles classified information will, with reasonable dependability, prevent:

- unauthorized (accidental or intentional) disclosure, destruction or modification of classified information;
- unauthorized manipulation of the ADP system which could result in the compromise of classified information.

To achieve these objectives the contractor is required to do three things.

- Prepare an ADP standard practice procedure. (ADP/SSP) describing the system and the security controls to be implemented for that system.
- Obtain written approval of the ADP/SSP from the cognizant security office prior to processing any classified information in the ADP system.
- Appoint an "ADP System Security Supervisor" for each facility with an approved ADP system, to be responsible for implementation of ADP security practices and procedures. Where there are multiple systems in a facility an "ADP System Security Custodian" may be appointed for each system processing classified.

The intent of this latter requirement is not to tell you how to manage your business by setting up new security positions. Rather, it's simply to ensure that these responsible assignments are made and are organizationally known and recognized. How you elect to accomplish these assignments is not the Government's concern. Our interest is that someone must have overall responsibility for implementation of ADP security, and that each system be supervised for operational compliance. This implies that the individuals must be knowledgable of the system for which they have been assigned responsibility. The System Security Supervisor, or the System Security Custodian working under the auspices of the System Security Supervisor, must investigate all reported security incidents to determine the cause and must identify corrective action that can be taken to prevent recurrence of similar incidents. Examples of the type of security incidents to be reported include:

- unexplainable out received at a terminal or work station;
- abnormal system response to user commands;
- inconsistent or incomplete security marking of printed output;
- unsuccessful attempt to log on from a remote terminal;
- extraneous data found in a computer listing.

The DISP is bound to the ADP security policy and requirements of the Department of Defense. In January 1973, a DoD ADP Security Manual was first published which established guidelines for techniques and procedures to be used to secure ADP systems. This manual became the basis for the Industrial Security ADP Security program. Section XIII of the ISM, Security Requirements for ADP Systems, was initially published in March 1976. Since that time there have been rapid advances in data processing technology and an exponential growth in the number of contractors, ADP systems and word processors processing classified data. Unfortunately, the rapid advances in technology

have been primarily made to effect processing efficiency, not security. This has resulted in numerous changes in our requirements, including a complete rewrite of Section XIII in May 1978.

Since there is no such thing as a sterotype computer system, Section XIII attempts to set down requirements applicable to any system that may be used in industry for the processing of classified information. Some of these requirements are quite explicit, while others allow broad interpretive latitude. Some of the requirements may seem quite realistic and reasonable to you, while others may not. Consequently, the security aspects of each system must be reviewed and analyzed in detail so that specific security requirements can be determined before allowing classified data to be processed.

Overview

Section XIII was written as an umbrella document covering all types of computer systems from the smallest minicomputer and word processor up to the largest ADP system. Therefore, the procedures and methods necessary to safeguard classified information are dependent upon the nature of the particular computer system and its use. It is the contractor's responsibility to safeguard all classified information contained in his system and assure that approved security controls are in place and effective. To accomplish this, the contractor must be thoroughly familiar with, and indoctrinate his personnel in the steps required to obtain an initial approval (in writing) from the Cognizant Security Office. This must be done before processing any classified information. The contractor must also be familiar with, and indoctrinate his personnel in the requirements for having his system reapproved if changes are made to his system or the area in which it is located.

Applicability

For the purposes of Section XIII, an ADP system consists of hardware devices and controlling software, as well as the environmental, personnel, and procedural attributes. The key word in automatic data processing ADP is *automatic* which connotes internally stored, self-directing programmable computers capable of performing repetitive processes with very little human intervention. This programmable logic can be in the form of software or firmware. The function of software and firmware is to control all hardware aspects of the system in the performance of the computer process. It is immaterial that the logic may be programmable only by the vendor, and not by the user.

The size of the system is also immaterial. Many small-scale mini-and micro-systems are on the market today, and each one requires controlling software, input/output devices, and storage modules, just like large-scale systems. They can be used for general purpose work, but often are used to perform special-purpose functions (e.g., word processing). Such systems may be found anywhere in the facility, not necessarily in an environmentally controlled computer room. While such systems as text editors and word processors may require much keystroking through keyboard input devices similar to typewriters, they are considered ADP systems because they store, format, and retrieve selected information on command and, in general, manipulte data, all under control of programmable logic.

Some office equipment can be characterized as computer systems in their own right. Document reproducers, memory typewriters, offline printing systems, computer output microfilmers, etc., have certain attributes of an ADP system (i.e., the ability to read and write magnetic media, internal memory and software controlled logic). Thus they are generally considered to be ADP systems, even though they may be more or less just transferring information from one media to another in a highly controlled atmosphere. Although security requirements for these systems may be similar to those for graphic arts, a system description document is still required. This documentation will not be as voluminous as for a large-scale computer system, but it must be sufficiently complete and accurate to describe the equipment and the security controls and procedures to be implemented.

While section XIII applies primarily to general purpose ADP systems, the security measures can also apply to computer systems which are integral or adjunctive to weapon systems, communication systems or tactical data exchange and display systems. The security measures to be employed for

these types of systems are normally established concurrently with the design and development of the system, utilizing the fundamental security concepts outlined in Section XIII. If the security requirements for such systems are not provided with the contract, the contractor requests guidance from the contracting officer. In the absence of guidance from the contracting officer, the provisions of Section XIII will be applied to the extent appropriate with the situation as determined by the local Cognizant Security Office.

Section XIII requirements are also applicable to classified computer processing that may be contracted out from one contractor to another. It also applies to government furnished ADP equipment used by a contractor for the performance of a specific contract. Section XIII does not normally apply to systems on user agency premises operated by contractors, where the contractor merely supplies bodies on a contract basis to run the user agency system located on the government installation.

Summary

As indicated earlier, the security requirements of Section XIII are based on a total safeguard approach, i.e., all facets of system protection must be considered — hardware, software, physical, personnel and procedural

Establishing security requirements in the DISP, becomes complex because of wide variations in the types of systems:

- Analog, digital and hybred (a combination of the two).
- General propose: designed to operate upon a wide variety of problems.
- Special-function: designed to operate upon a restricted class of problems.
- From the very simple to the very complex.
- Computers embedded in weapon systems.

Utilization of these systems in a classified mode also varies widely:

- from several hours a week to full-time;
- in any security mode-of-operation — dedicated, system high or controlled;
- in processing any and all levels of classified information — TOP SECRET, SECRET or CONFIDENTIAL.

While some portions of Section XIII may not appear to be realistic for your particular installation, remember that these requirements must specify all things for all contrctors, which includes many computer configurations and applications. The necessarily broad principles in Section XIII must be tempered by the specifics of each system and its particular environment, along with appropriate trade-offs, and the application of common sense, in order to satisfy the overall intent, which is clearly and simply, to safeguard classified information, contained in or handled by your ADP systems.

System Approval Process

The process of approving a contractor's computer system to process classified information represents a very difficult task. It includes an examination of the safeguards - hardware, software, operational procedural, physical, communications, and personnel, that have been provided and, ideally, a quantitative estimate of the probability of inadvertent disclosure of classified information. It is almost impossible to identify and protect against all possible security risks of a system. Nevertheless, in order to make the approval process meaningful, the security protection designed into a system must be quantified to the maximum extent possible.

The system approval process begins with preparation of an ADP standard practice procedure describing the ADP system and the security measures to be applied. The ADP/SPP is nothing more than a security manual for the computer installation. It's sort of the Bible of how the system will be used for classified processing.

From the approval point-of-view, the ADP/SPP is an indication of "how aware" the contractor is of the risks and threats associated with the operation of his system for classified processing. The ADP/SPP must cover not only security aspects of the system, but also configuration and processing aspects. This is to ensure that an adequate baseline exists that will permit a realistic judgement of overall system security. While the ADP/SPP is the basis for approval of the system, it is not necessarily the sole determining factor. Discussion with company management and technical staff, observance of system operation, past security history of the company, and other related pertinent information play in the evaluation.

There is no standard package of security requirements or safeguards which apply to all ADP systems. All the requirements in Section XIII can not be applied to every type of computer system on the market today. It's imperative that each system be analyzed in detail, considering the idiosyncrasies of that system and the safeguards necessary to ensure a resaonably secure system. Unquestionably, it's the contractor's obligation to safeguard classified information entrusted to him. Section XIII only identifies those areas of concern and establishes certain requirements that the contractor must follow in protecting those areas.

Only when security safeguards for the ADP system have been evaluated against Section XIII requirements, and judged adequate for the risks involved, can a system be considered approved and allowed to process classified data. This approval must be in writing from the Cognizant Security office.

When the system is approved the documentation should accurately describe the system and should serve as the basis for subsequent inspections. It must be recognized that some systems change frequently; and these changes may or may not have a bearing on the system approval. Therefore, any system change made relative to the provisions of section XIII (generally any change to the standard practice procedure) must be reported to the Cognizant Security Office for evaluation and possible reapproval. The same expertise is used for reapproval as is used for initial approval.

To prevent undue delays in utilizing the system for classified processing, development of the ADP/SPP should be initiated as early as possible. Cognizant Security Office personnel are there to assist and advise the contractor in its preparation. Our approval process encompasses the team concept whereby the local Industrial Security Representative is primarily concerned with area controls, personnel controls, and document controls. The Region Computer Specialist reviews and evaluates the overall ADP/SPP in accordance with the requirements of Section XIII of the ISM-with emphasis on the hardware, software and operational procedures before, during, and after classified processing. This approach has been the most practical and productive for both industry and government.

Inspections of all approved ADP systems are performed by Industrial Security Representatives during normal inspections of the facility.

When we inspect an ADP system at a contractor's facility, we are inspecting his actual operations against what has been documented and approved in the standard practice procedure. All ADP inspections are conducted by Industrial Security Representatives and not by computer specialists. When an ADP system has been reviewed and approved by the computer specialist, it lies totally in the hands of the Industrial Security Representative. The computer specialist serves as a technical advisor, gives technical assistance to the Industrial Security Representative and may sometimes assist in the inspection of large systems.

The number of ADP inspections performed are not as important as the quality of the inspections. During an inspection the Industrial Security Representative reviews the classified ADP system operations against the provisions of the approved standard practice procedure. Any changes or discrepancies in the procedures are discussed with the security manager, ADP system security supervisor, operations personnel, and others as may required. Serious discrepancies are reported.

Discrepancies deemed sufficiently grave are cause to recommend that operations of that particular ADP system be halted until the discrepancies are satisfactorily corrected. Our policy also states that if a contractor has not processed classified data on an approved ADP system during the previous 18 months, approval of the system may be withdrawn by the Cognizant Security Office and inspections terminated. The contractor is notified by letter of the withdrawal of approval. All documentation pertaining to the approved system is retained by the Cognizant Security Office for a period of 12 months to facilitate, if necessary, any need for a reapproval. This procedure was adopted as a cost-effective measure for both the contractor and the government.

ADP Standard Practice Procedure (SPP)

The documentation for a computer system processing classified data is an extension of the SPP required in paragraph 5s of the ISM. It can be a part of the facility SPP or a separate document

entirely, but it must be comprehensive and accurate or it will be returned to the contractor for additional information.

Whether the ADP/SPP is a stand-alone document or part of the facility SPP is the perogative of the contractor. If the ADP/SPP is a stand-alone document, then the facility SPP need only identify the existence of the companion document, and that it will be maintained on a current basis.

The format of the ADP/SPP is not a controlling feature of the approval process. Paragraph 112 levies the documentation requirements and enumerates them in sufficient detail to allow the contractor to develop a suitable document upon which an approval can be based.

An adequate system description document is the heart of the approval process and must describe the particular system and its idiosyncrasies, including its environment, capabilities, constraints and utilization. The documentation is also written for contractor personnel who are involved with the system. Therefore, it must be understandable to them as well as to the Government representatives. It's the responsibility of everyone of the users of the system to know about it and to follow its procedures and safeguards.

Sometimes asked: Is an ADP/SPP required for each and every system? Generally, an ADP/ SPP is required for each ADP system. However, if several ADP systems within a facility are duplicates of each other in all major aspects, and are operating in similar physical environments and are using the same procedures and audit trails, a single ADP/SPP covering all the redundant aspects may suffice. An addendum or supplement to this basic ADP/SPP can specify the location of each system and denote any idiosyncrasies or non-standard features and procedures of any one of the systems.

After approval is granted, if significant changes are made affecting the security features of the system, it must be reapproved. Significant changes are generally defined in paragraph 103a, but specific changes requiring reapproval are dependent on the particular system. The system reapproval process becomes rather academic if the contractor submits all changes to the ADP/SPP as required, or if changes are denoted during the inspection. In either case, the changes must be evaluated by the Cognizant Security Office, and the system is either still approved for the processing of classified data or is not approved until required changes are made in the security measures.

ADP/SPP Guideline

Two guidelines are available to assist in preparing the SPP. We encourage the contractor to use these guidelines. One of the guidelines applies for any type of computer system to be used in a classified environment. Another shorter and simpler guideline, was subsequently developed for word processors. The overall guideline consists of 13 major sections. There are questions and statements within each of the sections that paint a complete and accurate picture of all aspects of the classified processing activity. The guidelines necessarily contain sufficient details to develop a suitable system description document for any type of computer system-from a simple word processor to a large-scale general -purpose computer-processing any and all levels of classified information. Only the portions that apply to the particular system, its environment, and its specific method of operation need to be addressed.

In ADP security in the DISP, it is a continuing challenge to keep Section XIII up to date. Accelerating technology and the tremendous growth in the use of computer systems for classified processing, have made it necessary to continually review and update ADP security requirements in the Industrial Security Program.

Some figures will indicate the magnitude of the challenge. When Section XIII was rewritten in 1978, the typical ADP system used in classified processing was the large general-purpose computer located in a centralized installation. At that time, about 500 such systems were approved to process classified information. It was estimated then that perhaps there would be 1,000 approved ADP systems in our program today. Now there are over 4,600 approved computer systems processing classified data in over 1,000 contractor facilities, with more systems being added all the time. The major factor in this explosion of ADP systems

has been the recent trend from the large centralized computers to the minicomputers and word processors that are more conveniently located in the immediate workplace. This trend has significant implications for ADP security.

To meet the ADP technological and operational change, Industrial Security Program personnel must work closely with industry. A working group recently was formed to provide interaction , and to review our existing computer security policy. This group sponsored by the Industrial Security Committee of the Aerospace Industries Association is composed of ADP security experts from industry and government and is tasked with identifying and recommending procedural and policy changes consistent with computer technologies of the 1980s that will improve contractor productivity, possibly result in significant cost reductions, and also be in balance with our security objectives. The group began their efforts in February. Any proposed changes to the ISM will be coordinated with members of the industrial community before being submitted to us early in the fall. This joint industry/government effort will assist us in keeping our policies for ADP security realistic, workable and cost-effective.

Protection of Software and Data

Section XIII prescribes the security controls that should be implemented for system software, classified application software, unclassified application software, and data that is used in a classified environment. A brief explanation of this change is as follows:

1. **System Software (Operating System).** The contractor is required to have a dedicated copy of the operating system that is used exclusively for processing classified data. Even though the operating system itself is not classified, the software must be safeguarded as though it were classified to the highest level of data that will be processed by the system. This requirement is necessary and includes software obtained from sources outside the facility as well as that developed by the contractor personnel. These safeguards must be established at the earliest feasible time.
2. **Classified Application Software.** The protection of this type of ADP software has been in the manual for some time. This change further explains the requirements for the protection of classified application software and emphasizes the controls that must be maintained during the time such software is used, removed and stored, as well as the internal marking of the classification on the storage media.
3. **Unclassified Application Software.** This change now allows the development and use of unclassified applications during the time classified data is being processed provided that:

- the unclassified software is introduced into the system in a read-only or write-protected manner;
- the classified software and data is reviewed, approved, and authorized by appropriately cleared and knowledgeable contractor personnel, or
- the contractor has developed standard configuration controls and service management procedures to assure protection of classified data. These procedures must be approved by the Computer Security Specialist in the Cognizant Security Office.

ISR Update. Currently the Industrial Security Regulation (ISR) contains no information on security requirements for ADP systems. A new section will be established in the ISR that will summarize the ADP system security requirements and provisions of Section XIII on the ISM.

Requirements of the ISM must be applied uniformly, and with the exercise of good judgment considering the hazards which can reasonably be expected to prevail in any given case. To attempt to apply safeguards against that which is *possible* versus that which is *probable and reasonable* is not only futile but is a disservice to our responsibility for maintaining a creditable program. The net result would be a program which totally ignores cost/benefit analysis, threat assessment, operational realities, and would adversely impact on both industry and government.

ADP SECURITY PROBLEMS AND SOLUTIONS

Carole Jordan
Air Force's Eastern Space and Missile Center

I've been involved with computers for about 16 years, but I didn't know about security until 4 years ago. I programmed and did systems analysis work for The Defense Systems Automation Center in Columbus, Ohio. My work was mainly in the area of telecommunications. I and my coworkers designed computer systems in a laboratory environment using test data. After our various systems were tested, we installed them in all of the centers, depots, and Defense Contract Administration Service Regions (DCASRs) around the country.

As with any good software development center, the emphasis was placed on accuracy and efficiency. An important feature of any software system is to serve the user as fast and accurately as possible. The idea of anyone using the system for anything other than what it was intended was not given much consideration until the mid-70's.

Things started changing at the center. Now security is considered during the design stages of new systems and is added into current systems. Various controls are being built into systems to prevent or detect unusual occurrances such as deliberate or accidental user manipulations of the information.

I and my coworkers were responsible for our own programs while they were in use around the country. Any programming that provided for user input mistakes was done voluntarily on our part to avoid being called in, sometimes in the middle of the night, to create a cure for a hung program somewhere.

I was primarily responsible for my own programs, and I was an alternate for one or two other programs. I was called in at night on the fourth of July weekend. Someones program had caused the system to hang at Defense Personnel Support Center in Philadelphia. It took hours to figure it out, but the answer was simple. The program was inpecting input records from another program containing either a 1 or a 2 in the first character of each record. The programmer had planned the logic to read: If the input is a 1, go this way and do certain processing; otherwise go that way and process. No provision was made for any other input type. The program that ran before the hung program produced one record with a character other than a 1 or a 2. It produced an 'A' record erroneously. I formulated a "quick fix" solution to make the program run by changing the logic to: If the input is a 1, go this way and do certain processing; if the input is a 2, go that way and process. Otherwise reject that input record and get another input record.

I am providing the detail of this event to demonstrate the implications of an oversight, a wrong assumption, or carelessness on the part of a programmer. In the 1970 environment —when an error occurred — a user could create the input records but had no control or awareness of the processing until he received the output products. That was called a batch environment as opposed to the distributed on-line systems of today. In today's world of computers more users are directly associated with the processing of information. A user at a remote terminal has more power than ever before. Today, the users are different.

Suppose a terminal user is taught to input a record starting with a 1 in order to update a certain record in a file. And suppose he is taught to input a record with a 2 in the first position to cause a printed report to come out.

If the careless programmer had not provided for errors on the part of the terminal user, the user might disrupt an entire computer system by inputting a record with an 'A' in the first position. That is only one possibility. A careless programmer can leave a door open for a user. What if the programmer's mistake causes a properly cleared user to access classified records or files for which he had no need-to-know? This mistake may never be found unless the user voluntarily makes the fact known! Do you see the implication?

Computer security is a people problem. Don't be confused with all the hardware in the computer room. The greatest threat is from *within*. Mistakes or oversights may cause classified information to be subject to compromise. Mistakes can usually be detected. But intentional attempts to jeopardize

classified information can be difficult to protect or detect. How authorized users and system support are handled and controlled is the single most critical part of the ADP security program. People must be held *accountable for what they do* because people who have access also have opportunity.

A *user* is someone who has access to the resources of a system, and is capable of updating a file, creating or destroying data, or creating output products such as printed reports. A *customer* can request output products but must interface with a user who is his go between to the ADP system. A *system support* person works in the computer room, accesses the control console, turns on the system, mounts tapes, and marks output products.

What is the threat and what can they do? The Law Enforcement Agency is involved with hundreds of cases each year relating to computer crimes. These are the intentional crimes, not the accidental ones — unless someone takes advantage of the accident for personal gain. The Law Enforcement Agency has compiled statistic to help identify the common situations that precede a particular crime. Law Enforcement Agency's statistics have developed a profile of the typical criminal: He may be young, attractive, clean shaved, intelligent, and he could be employed in a white collar, technical job with authorized access to the resources of a company and its computers.

What can a user do:

Users (programmers) can:
- cause accidental errors
- write-in extra routines
- copy and sell the software

Users (data input and remote terminal) can:
- accidentally or intentionally destroy data (delete)
- accidentally or intentionally make errors in updating
- copy information for their own use
- enter false input data

System Support Personnel can:
- copy and steal data and software
- accidentally or intentionally destroy data

How can we reduce the threats by preventing or detecting security incidents? There is no single answer. Some possibilities are to devise Collection of Security Controls tailored to your system —hardware, software, personnel, and administrative. Physical and personal security by itself is not enough. Granting blanket need-to-know is too simplistic a solution. Always be aware of the following:

- Do not depend upon software security controls entirely. They can be bypassed. Passover systems can be broken. Competent programmers can write their own access routines.
- *Do not depend upon the ignorance of the* user. People do not remain ignorant. They *will* acquire the expertise needed to overcome any control that was based upon ignorance.
- Some threats cannot be completely *prevented*, but they may be *detected*.

Developments in computers that effect security: Office automation has arrived. On-line (real-time) remotely accessed systems have replaced batch-oriented systems for the most part. There are word processing, distributed processing, data bases, intelligent terminals, minis, micros, and personal computers. The increased power to the user requires an increased need for audit trails and user identity.

Many traditional security controls that were designed for large computers are not adaptable for small computers. For example, closed areas may not be feasible; a small computer may not justify two operators on duty; software programmers may not be excluded from computer rooms if the same person is programmer, operator and user; and it is easier to tamper with the system log or the password controls.

Some advice for word processors or small computer security:
- Follow the ISM (Section XIII) just as if it was a large system. Capabilities grow while the hardware becomes smaller.
- Talk to your local DIS Representative and computer specialist. Physical controls are going to vary depending on the location, and the type of computer.

- Watch out for a word processor with an erase button or feature, or a non-removable memory device, or non-volatile.

Some deficiencies that occur in ADP security are:

Lack of management support which results in a "low profile" security posture. Characterized by lack of adequate resources and funding in the security department.

People on the access list to the computer room who have little or no need to be there.

Audit trails inadequate, not understood and not reviewed.

Inadequate or non-existent memory-clear routines

No software protection, especially no protection of software that clears main memory or disk packs.

Abusing the privilege of using the computer room Closed Area for open storage of classified information.

Declassification procedures not established or not used, especially in the event of a damaged disk pack or replacement of core memory.

Inadequate control over tape and disk libraries and over working tapes.

No working relationship between the data processing areas and the security office.

Complete trust in the data processing department to follow established security procedures in the face of more expedient alternatives after they have carefully weighed the probabilities of getting caught by the security people.

Finally, when you have obtained approval, don't get complacent. A self-inspection amd the regular DIS inspection may reveal that the security controls don't work as well as planned. Security effectiveness depends on awareness and attitude as well as hardware, software, physical, personal security, and administration control. A real security program takes *effort* on the part of management, the data processing people, and the security office.

APPLYING DERIVATIVE CLASSIFICATION

Edward Smith
Defense Industrial Security Institute

I'm going to talk about applying derivative classification. The title on the agenda is slightly different.

I'll discuss primarily what we discuss with most of the people who come to the course in Richmond. Many people know very little about what applying derivative classification means. They understand that it's not creating an original classification, and they know that security people in the United States Government, from time to time, apply derivative classification.

The first thing I try to explain is that it's very fundamental, and it's very logical. Most people think that when they have a source document and they extract, for any purpose or reason, any information contained in any classified paragraph or portion of a source document, and they transfer any part of that information down through their derivative document, that they merely transfer the classification along with it. I try to explain that there is more to applying derivative classification than meets the eye. Certainly basically this is true.

The act of applying derivative classification is a logical consideration of the information that you're dealing with. I indicate that everybody has at one time or another prepared some kind of a paper, either in high school, a secondary school, or a university (perhaps a term paper or a thesis), and everybody understands the science of doing classic research.

At the library are sources of information that suit the purpose of the job to be performed. Extract that information from the various sources, whether printed documents, or communication media, such as films, microfilms, electromagnetic tapes, and so

on. In derivative classification, we select the information we need, and we apply it in our own document. The only difference is in applying derivative classification, we have to classify it; and we try to classify in accordance with the intentions of the original classification authority. The idea is to accurately reflect the classification intentions of the original classifier.

Many people look at the viewgraph or a slide and say, "All right", this is all very logical. I extract information from paragraph 2 of source document C and transfer it down into paragraph 4 of my own derivative document, and I transfer the classification right along with it." But there's more to it than that. The first thing I ask is, "What does that TS there in front of paragraph 2 of source document C really mean?" Can anybody tell me? What does that TS mean? Or what does that S mean in front of paragraph 5 of that same document, or the C over in paragraph 1 of source document A? Can anybody tell me accurately what that means? (See Enclosure 1)

Response: Some of the information in the portion is classified as indicated.

Mr. Smith: That's exactly right. But most people feel that all of the information contained in that paragraph is classified at the level that's included at the beginning of the paragraph. I say it a bit differently. I say that it represents the highest level of any classified information contained in that particular portion or paragraph of the document. This is hard for people to understand. Many people say, "I've been doing it for years. I've never had any repercussions. I merely transfer the classification along with the information." (And they go on to discuss that fact,) but let's assume for a minute that paragraph 2 of document C is a very complex and long paragraph containing 25 sentences and perhaps as many as 30 or 40 different ideas. The idea is that instead of extracting the entire 25 sentences, we only extract perhaps two, three, or four sentences out of that particular paragraph. Do we know for certain that we've extracted classified TOP SECRET information? Certainly not. Could it have been SECRET information that we extracted?

Question: Do we know for certain that we didn't?

Mr. Smith: No, we don't. No, we surely do not know for certain that we did not. But it could have been TOP SECRET; it could haave been SECRET: it could have even been CONFIDENTIAL, couldn't it? And it might all be unclassified information.

Question: Right, but since we don't know whether it is TOP SECRET, SECRET, or CONFIDENTIAL, then do we have a choice to do other than make ours TOP SECRET?

Mr. Smith: Tell me, do we?

Response: I'm saying no. Not unless I have other classification guides available to me.

Mr. Smith: That's the heart of the matter right there. And that's the point that we can't get through to most people who do in fact derivatively classify. About 80 percent of the people that come to those sessions who apply derivative classification tell me, "But we never have classification guides. They're just not available. What is a classification guide? I've been doing this for three years. We don't have a guide. I've heard of guides, but I know nothing of them."

You hit it right on the nose. There is really no way of ensuring that the particular information that you extracted from that paragraph is in fact classified at the level you hope it to be. But suppose you're derivatively classifying; you don't have a guide; you don't know how to get a guide; and you've got to get this job done. What are you going to do?

Response: I make it TOP SECRET.

Mr. Smith: You're darn right you're going to make it TOP SECRET. Would anybody have the guts to do otherwise, no matter how you felt about it and no matter how intimately you were associated with the information contained in that document? Would anybody have the nerve to just arbitrarily change that classification? Mr. Irving Boker could assure you that he has no right to do that. He has no authority to do that. In fact the extent of his classification guidance is contained in those derivative documents, that's what he's going to put. Isn't that

on. In derivative classification, we select the information we need, and we apply it in our own document. The only difference is in applying derivative classification, we have to classify it; and we try to classify in accordance with the intentions of the original classification authority. The idea is to accurately reflect the classification intentions of the original classifier.

Many people look at the viewgraph or a slide and say, "All right", this is all very logical. I extract information from paragraph 2 of source document C and transfer it down into paragraph 4 of my own derivative document, and I transfer the classification right along with it." But there's more to it than that. The first thing I ask is, "What does that TS there in front of paragraph 2 of source document C really mean?" Can anybody tell me? What does that TS mean? Or what does that S mean in front of paragraph 5 of that same document, or the C over in paragraph 1 of source document A? Can anybody tell me accurately what that means? (See Enclosure 1)

Response: Some of the information in the portion is classified as indicated.

Mr. Smith: That's exactly right. But most people feel that all of the information contained in that paragraph is classified at the level that's included at the beginning of the paragraph. I say it a bit differently. I say that it represents the highest level of any classified information contained in that particular portion or paragraph of the document. This is hard for people to understand. Many people say, "I've been doing it for years. I've never had any repercussions. I merely transfer the classification along with the information." (And they go on to discuss that fact,) but let's assume for a minute that paragraph 2 of document C is a very complex and long paragraph containing 25 sentences and perhaps as many as 30 or 40 different ideas. The idea is that instead of extracting the entire 25 sentences, we only extract perhaps two, three, or four sentences out of that particular paragraph. Do we know for certain that we've extracted classified TOP SECRET information? Certainly not. Could it have been SECRET information that we extracted?

Question: Do we know for certain that we didn't?

Mr. Smith: No, we don't. No we surely do not know for certain that we did not. But it could have been TOP SECRET; it could haave been SECRET: it could have even been CONFIDENTIAL, couldn't it? And it might all be unclassified information.

Question: Right, but since we don't know whether it is TOP SECRET, SECRET, or CONFIDENTIAL, then do we have a choice to do other than make ours TOP SECRET?

Mr. Smith: Tell me, do we?

Response: I'm saying no. Not unless I have other classification guides available to me.

Mr. Smith: That's the heart of the matter right there. And that's the point that we can't get through to most people who do in fact derivatively classify. About 80 percent of the people that come to those sessions who apply derivative classification tell me, "But we never have classification guides. They're just not available. What is a classification guide? I've been doing this for three years. We don't have a guide. I've heard of guides, but I know nothing of them."

You hit it right on the nose. There is really no way of ensuring that the particular information that you extracted from that paragraph is in fact classified at the level you hope it to be. But suppose you're derivatively classifying; you don't have a guide; you don't know how to get a guide; and you've got to get this job done. What are you going to do?

Response: I make it TOP SECRET.

Mr. Smith: You're darn right you're going to make it TOP SECRET. Would anybody have the guts to do otherwise, no matter how you felt about it and no matter how intimately you were associated with the information contained in that document? Would anybody have the nerve to just arbitrarily change that classification? Mr. Irving Boker could assure you that he has no right to do that. He has no authority to do that. In fact the extent of his classification guidance is contained in those derivative documents, that's what he's going to put. Isn't that

right? And if he does anything else, whats he doing? He's acting in place of any original classification authority. If so, he's doing something that he has no authority to do; he's acting as an original classification authority.

If anybody has read through Irv's tomes (and I'm sure many of you have poured through them and know exactly what's contained in them). You will realize that we were particularly concerned with the one about the DoD classification management system. I've read that over and over and over again, and I can't couch it in the terms they used in that document, but what I seem to read in the bottom line of that document is that the DoD classification management system, particularly as it applies to derivative classification, is in a state of choas. Did anybody get the idea that everybody's doing their own thing?

I say to people in my class, "You don't have a guide. You don't have anything to guide you at all. How do you make such a decision?" I've had people say things like this to me. "Look, I've been in this busineee for 6 to 8 years. I can feel it in the pit of my stomach. I know." Oh they say, "My supervisor has been advising me on that. He said no matter what kind of a document you prepare, just stamp SECRET at the top and bottom of each paragraph." I did that. I used to be with Army Intelligence years ago. I remember I used to write reports by the hundreds. All I needed to know about classification was that my boss said, "No matter what it is you write, just stamp this little caveat at the top. and stamp everything SECRET." Everything was SECRET. It didn't matter what. So that was the extent of my understanding, and I really never thought beyond that. I said "Well, this fellow knows. He's the boss. He ought to know what's classified and what isn't."

When I finally found out that there was such a thing as classification management, I was absolutely astounded. I never learned it until I got into the Industrial Security Program. I left the Army Intelligence Command and went with industrial security, and I started immediately. I encountered classification guides. I said, "What is this on all these matters?" It meant nothing to me; and for the longest period of time, it just seemed like a lot of nonsense.

Now, the evolution has been completed. Today, I cannot understand how anybody can do any kind of a job of applying derivative classification without the benefit of a classification guide. I can't see how it can be done.

You saw the initial problem there, the idea that who knows whether that's TOP SECRET up there? Who knows whether this is SECRET? And there are a lot of other problems that you will encounter. How about the dates of those documents? It's entirely possible that some of them may be dated five or six years ago, but they still contain research information that you need in the course of your job. In the performance of your duties, you need the information contained in that document because the information pertains directly to what you're doing. What can you do beyond that point? You have information that may have been downgraded. Of course, that's just about out the window, And even the application of declassification probably won't have much applicability in the future, not as much as it has in the past.

The point is that up until this time, it played a very important role. Frequently the classification of the various elements of information in older documents became downgraded and declassified. So if the document was dated 1978, who's to say that the information, even if every word in that paragraph were TOP SECRET then, that it's still TOP SECRET today? So what's the answer? We've already talked about it. It's the classification guide. We really hit hard on the classification guide.

Now I know most of you are involved with industry. And I know the DD Form 254. Before my employment at Richmond, I was a classification management specialist at the Defense Contract Administration Service Region (DCASR), Cleveland, for about four years. That was my job, so I know the 254, and I know the problems encountered with the 254. However, what we're concerning ourselves with here primarily is item 15 on the 254 — the item that gets less treatment than any other item on that form. I think it's the most important item. Item 15 contains the classification specifications and the security required for that particular classified contract.

I know what the situation was 10 or 12 years ago when I was doing it. I'd get a 254 and every block appeared to be filled out exactly right. I'd come to item 15 and see two or three lines contained in item 15 for a classified complex project that might have been performed by the Goodyear Aerospace Company in Akron or the Battelle Memorial Institute in Columbus. These were highly technical classified projects and the classification was contained in two or three lines. "All the information on this project is classified SECRET," or something like that, with a few other specifications. This bothered me, but I didn't know what to do about it. Now I am very happy about the trend that has developed with DD Form 254. I believe Mr. Bob Green was saying that only that classified information that pertains to that particular contract should be contained on a DD Form 254. And I agree with that. The trend today is that they are actually attaching those portions of the classification guide, the original guide, along with the DD Form 254. I like that trend.

That's why we stress the fact that in order to properly derivatively classify, you must have a classification guide or a DD Form 254. It says specifically in the DOD 5200.1R and probably in the Industrial Security Regulation Manual, that every derivative classifier is obligated to make every attempt to verify his derivative classification.

I ask people, "How do you verify a derivative classification?" Nine out of ten will say, "You've got to contact the original classification authority if you want to verify it." Is that right? Can you imagine what it would be like on major complex weapons systems, if the office of original classification authority sat there and verified every derivative classification decision made on a project. It's impossible.

So when you have the most recent copy of the classification guide or the DD Form 254, you are in a sense directly communicating with the original classification authority. And if that guide is written properly, accurately, concisely, there shouldn't be a problem. That's why I made that statement earlier and I'll make it again. I cannot see how any project can progress, as far as the classification of that project is concerned, without the use of the classification guide, because when you see it in the guide, it's listed in very short, direct statements. There should be no question about what's classified. But if you try to pick it out from a narrative paragraph included in a derivative document, it is almost impossible to determine the classification aspects of that paragraph. So we stress this again and again at Richmond, and that's why we feel so strongly about it.

I'll tell you frankly that up until about four years ago, we didn't even discuss derivative classification. As a matter of fact, eight or nine years ago derivative classification was a dirty word. We weren't permitted to use the word. You did not use the word derivative, derivative classification. I never could find a word that fulfilled the meaning of that word. There was no emphasis on derivative classification, and again everybody was doing his own thing.

I'm afraid to have to tell you that from what I can ascertain from discussion with hundreds of people who attend our courses every year, the problem is still there. It still exists. All we're trying to do is evangelize a little bit if we can, to try to get people who can understand that we're saying to go back and tell those people in their facility what we mean, what it's all about. It is so simple, straightforward, and logical that I can't understand what the problem is. But it *is* a problem.

Comment: What you say makes a lot of sense, but it assumes that the derivative classifier has instant access to the classification guide. That's not always the case. If you have a problem getting the letter off or the documents off, and you can't wait to look it up in the index and order it, what do you recommend?

Mr. Smith: You should do prior planning. The idea is that if you're going into a project like this, before you get into it, you should prepare. And on every classification guide that I've seen, it says on the guide "local reproduction of this guide is authorized." Doesn't it say that in most cases? Don't you encounter that? Don't you think DoD has gone a long way in this respect as far as that index is concerned? You know you're going to bid on a contract and you're concerned with particular projects — of course, it's a little bit different. I know that the contractors are not authorized access to

that DoD index which has often been a source of wonderment to me. But I guess the idea is that if a DoD contractor needs access to a DD Form 254 classification guide, he's suppose to work through his classification management specialist or the contracting officer. I understand that. But I feel that a lot of that kind of thing could be avoided if the involved organization plans ahead. I know situations arise where you have to know now. And if we can't get adequate guidance, you and I are going to have to make a decision. And our decision in some cases may be better than the decision of the original classification source. That doesn't mean we have the authority to do that though, does it? No, it doesn't. All right. I think that's enough said about applying derivative classification.

Comment: There's more information.

Mr. Smith: Okay, there's more information. That's right, but it doesn't mean that we haven't in fact captured any classified information, sensitive information, and transferred it. It's true, there is more information there. But just based on the information contained in paragraph 3 of the source document, have we in fact properly transferred the classification or the sensitive information?

Comment: No.

Mr. Smith: People say no. I heard others say yes. Who says no, we haven't in fact?

Comment: I say no.

Mr. Smith: Tell me why, would you please.

Comment: Because obviously in the source document the two figures are what's classified, the 6,000 pounds and the 183 degree arc. And I'm not putting that in my paragraph. (See Enclosure 2)

Mr. Smith: Now Liz said it's obvious to her that the classified information, the sensitive information in that paragraph are the numerals there, that the tensile strength of that guidewire is 6,000 pounds. She also says the fact that the flexibility of the wire obtained an arc of 183 degree in an eight-inch diameter, circumference, whatever it is there. That is the obvious classified information to her. Well I would say that you've got to be at least partially right because there are really only two ideas in that paragraph, aren't there? One of them concerns tensile strength. The other one concerns flexibility.

Comment: Doesn't it depend on your contractor talking about 254s, what the 254 says?

Mr. Smith: Will you just explain a little bit more what you mean?

Comment: I'm aware of contracts where a widget is classified under this contract CONFIDENTIAL, and in this contract it's UNCLASSIFIED.

Mr. Smith: Well, what is that? What have you got when you've got that? Should we have those kinds of situations? That's inconsistency and Irv Boker had enough of that, I'll tell you that, to satisfy me. And that's what I'm trying to avoid here through the use of the classification guide. Now it's true, that's possible. The Air Force might call this CONFIDENTIAL and the Army might say it's SECRET and the Navy in turn, I don't know whether it's classified. That's possible. I agree with that. But let's just assume for moment that the classification as it's contained in the guide is correct. Remember this. The art of doing original classification guides is a very subjective thing. Is is not? There's nothing objective about it at all. We don't have any formulas for it. We can't take this from that and come up with this every time. It is in the mind of the individual who is required to make the decision. It's a strictly judgement call. We've selected the original classifier because we believe he's the most experienced, the most imaginative, perhaps the most intelligent person we have available to do the job. He's more intimately related to the information contained in that project than anybody else. And even at that, he's not always qualified to make all classification decisions. As I talked with Mr. Bob Green about it the other day, most classifications today on complex projects are made as a result of consensus. People sit together in committees or groups and discuss this. I can remember talking to the gentleman who was an original classifier on the Naval sea system, and he said on one issue he sat for two months and argued with an engineer about the classification of one element. Finally they reached a consensus. So there's hardly anybody today, if he exists at all, who is sufficiently knowledgeable to make deci-

sions concerning every classification in a very complex project so it's done by consensus. And it is a subjective thing. If five of us say that's SECRET and the other guy says, "I think it's CONFIDENTIAL," more than likely we'll opt for SECRET. Is that right? And that's logical.

Comment: It seems to me without the classification guide on a specific subject, you can't tell in your derivative document whether you've got classified information or not.

Mr. Smith: Right, but this is the moment of truth. You are it. Make the decision, my friend. You have no guide, and you have no time to get the guide.

Comment: Without the guide, you cannot do anything....

Mr. Smith: You've got to make the best judgment you can make. You're not going to send that document out unclassified, are you? You're going to make a judgment. Either you're going to say, "Yeah, I think they have done this. I think that this is the case," or you're going to say no. We've already dealt with that. How many of us are going to stand up here and say, "No, that's not classified information." You're not going to do it, are you? You certainly are not going to do it. So your decision....I know what your decision is because it's the same as mine. You're going to call it CONFIDENTIAL. Isn't that right? Sure you are. But have we done it correctly? That's the question. Now that's fairly straightforward. It's easy to see there. We talk about tensile strength. We all understand what that is. And we've talked about flexiblity. We understand what that is, don't we? Now let's turn over the page. We've got another paragraph added to this thing right here now. We've got source document 2 as you can see on that side, and we've added paragraph 5 to our derivative document and we've got to classify paragraph 5 if it's appropriate. We believe we've got some essential elements of information from paragraph 1 of source document 2, and I believe that I've transferred those sensitive elements over to paragraph 5. Read those paragraphs and tell me about it this time. It's not quite so easy this time. Now does anybody want to raise his hand and speak up assertively and with certainty concerning the classification decision made in this case? How many of you can answer that? Now the definitions become very nebulous, don't they, and a little bit unclear. And the terminology is...I'm not sure I'm familiar with all that terminology. I've known what tensile strength is since high school, and all of you have probably or most of you have. But the rest of you.....And also, we all know what flexiblity is. But what's a PMPSRQ-689 subsystem, folks? Or how about an impulse rate? What do you think? All you can do is give me a guess, is that right? (See Enclosure 3)

Comment: Yes.

Comment: I believe from the source document you can take the subject of that paragraph. You're establishing some parameters. In order to achieve some parameters, you included some other capability. That apparently is what made it classified, isn't it, apparently?

Mr. Smith: Yes, that's right.

Comment: And if you read the derivative document, you're not talking about parameters. You're not giving away apparently the specific technique or subtance to be used to achieve it. Therefore, it may well be at a lower classification or unclassified.

Mr. Smith: Or unclassified. Any of you other folks feel that way too?

Comment: I would think that the model there was relating to capabilities, relating to some equipment. That to me means a primary classification, the fact that this R process allows you to do an unusual type of coding. The derivative paragraph expands on that capability.

Mr. Smith: Yes, it does. It's possible, is it not? It's only possible, but then you think about the only place you'd go would be to TOP SECRET. What this I think does prove is this. Not only....we haven't gotten to this point. We're going to get into a classification a guide on this. I think that the way to look at this in my estimation is that the're about four or five or six ideas over there in the left hand paragraph and I want to know have I really transferred any of those ideas over here. If I have transferred any, then I think I have to assume that it was classified SECRET. Now your idea is that we've created something more than was included in the first paragraph, the original paragraph. And that's

entirely possible too. But we've got the idea....first of all, we're talking about PMPSRQ-689 subsystems. Could that fact itself be classified, the fact of the existence of such a thing? Possibly. No certainty on that because, first of all, what does PMPSRQ-689 mean to anybody without any other information?

Comment: DOD...required to be UNCLASSIFIED.

Mr. Smith: Okay. So then we'll say that's not classified. I'll buy that. I'll accept that. He says you're not allowed to classify that kind of nomenclature. It's just an alphanumeric symbol and it doesn't mean anything, and I think he's right. Taken out of context, it certainly wouldn't mean anything to anybody. Now we talked about the fact that we've got...let's see, in order to establish electronic power measure parameters for this thing, we had to use an R pulse processing rate with it. Now the idea is that to you and me that might not mean anything, but to somebody who is specially schooled in this kind of thing, they might have great meaning.

Comment: anytime you establish power measures, you're....

Mr. Smith: Okay, so it might be that. And have we transferred any of that idea? Yes, we have down there. We talked about that down there. We also talk about an R pulse rate. That idea itself might be classified. And then we talk about the fact that this enables the subsystem to sort out unusual coding parameters. And he said he felt that was sensitive, and he could very well be right. But the problem is at this point we're right back where we started. We can make an educated guess, albeit a highly-educated guess. We're all engineers and we're intimately involved with this information. But we can't say so without the classification guide. Now I just happen to have a classification guide along with this for these particular two paragraphs. We'll start on the first side there. You'll see the same thing up here that you've got again in your handout there. And this first paragraph deals with specifications for the guidewire, so that was paragraph 3 of source document 1. Now let's consider what we've got up here. First of all, it talks about the type of the guidewire. It doesn't matter. It's UNCLASSIFIED anyhow, as you can see. How about the composition? Do we dicuss the compostion? Not at all, but we can recognize instantly that compostion is classified SECRET. But we know we haven't discussed it. No problem. Capability, communications capability, how many electronic messages can be sent up and down this guidewire or how it's done. Do we discuss that at all? No, we don't. how about flexibility? (See Enclosure 4)

Comment: Yes.

Mr. Smith: Flexibility is discussed. Is it discussed in source document number 1, paragraph 3? (See Enclosure 2)

Comment: Yes

Mr. Smith: Is it discussed in derivative document, paragraph 3? No, it isn't, so it has no applicability here as far as that paragraph is concerned, right? Okay, how about playout speed? I think we all understand what that is. Anybody who's a fisherman knows what playout speed can mean.

Comment: I'm going to be honest with you.

Mr. Smith: Okay, backlash, whatever you want to call it. Okay, We don't discuss it anyhow. Weight per 100 meters of the wire. Any discussion? None at all. Tensile strength.

Comment: Yes.

Mr. Smith: Finally we get down....and it can be instantly recognized in this case that we have properly classified our derivative paragraph 3. Is that right? Because it says there that the tensile strength is classified CONFIDENTIAL. And I know my figures are not exactly accurate, but if 80 percent of 6,000 is 4,800, or whatever it is, then it's easy enough to figure out what 100 percent is. I don't think anybody would have any difficulty with that. All right, how about test velocity, test objectives, test schedules? Any discussion. Nothing at all, right? They're all UNCLASSIFIED anyhow. They have no applicability. How about this, test data, analysis, and conclusions revealing capabilities, limitations, weaknesses, or vulnerabilities of the guidewire? Did we discuss that? (See Enclosure 2)

Comment: Yes.

Mr. Smith: It's instantly recognizable, isn't it/

There was no way we really could know that before we had a classification guide. I wrote this thing. I set it up folks, let's be honest, for my own purposes and I think you can understand that. Turn over to the other side. just ignore overall performance. It has to do with the guidewire. Let's go on to the PMPSRQ-689. Is the mere fact of the existence of the PMPSRQ-689 classified? (See Enclosure 4)

Comment: No.

Mr. Smith: No, it is not. There's the answer to that. It certainly is not. Now we're getting down to the nitty-gritty here. It says spectral and frequency characteristics, and spectral and frequency characteristics are classified SECRET. Do we discuss spectral or frequency characteristics in our derivative paragraph? (See Enclosure 4)

Comment: No.

Comment: Yes.

Mr. Smith: If you asked me, do you know what I'd tell you? I don't know. I have no idea. As a matter of fact, I have a lot of people come to me in class and say, "Mr. Smith, I see you really know what you're... you know your apples when it comes to derivative classification. Will you come over to my office, sit down with me. I'm really running into problems with a derivative classification of these document I'm working on. I know I could handle the whole thing in just a very short order if you'd come over." say, "If you brought me over there, it would be like taking a babe in arms over there to apply derivative classification to your document." Why? Because I do not have intimate knowlege of the science or the technology or whatever it takes to understand and to work that project. I might understand a little bit about the mechanics of applying derivative classification, but that's all I understand, unfortunately. And I don't know if it can ever be any other way than that unless I sat down and spent a lot of time and tried to learn it. i don't know. But that's a problem that can't be answered. So I make the point that if you don't understand the material you're working with, a lot of items the classification guide will do you no good whatsoever. It will nto hep you. So I can't answer that question about spectral or frequency characteristics. Performance characteristics limitations. It's SECRET. We're talking about either theoretical or major data. How about that? Do we talk about theoretical or major data as far as performance characteristics are concerned? how many think so? I think so. This gentleman thinks so. He'd like to comment on it.

Comment: There's going to be impulse.

Mr. Smith: Less effective or something, right? yes. But are those specific performance characteristics?

Comment: Theoretical.

Mr. Smith: Well, now wait a minute. you say it's theoretical. But can't theoretical characterisitcs be specific?

Comment: Possibly.

Mr. Smith: So we're got a problem here. Now the problem is either the guy who has to do the derivative classification may not understand the information or there's something wrong with the guide, right? That's where the fault lies. Let's go on and look at the next one. System capacity. It says it's SECRET information disclosing multiple signal handling capacity. Are we home free this time?

Comment: No.

Mr. Smith: Why not?

Comment: It's two. It's dual.

Mr. Smith: That's not multiple. Okay, that's just dual. Is that what you mean?

Comment: That's more than one.

Mr. Smith: More than one — that's multiple. So we are home free then.

Comment: No, we're not.

Mr. Smith: Why not?

Comment: It says if you disclose this multiple signal handling capacity, it's SECRET.

Mr. Smith: And we classified that paragraph

SECRET. So we're home free. That's what I mean.

Comment: We classified it CONFIDENTIAL.

Mr. Smith: Oh, did we? Wait a minute. Is that paragraph 5?
Do we understand each other on that? Anyway, that's what happened there. This has always satisfied me except some smart guy in one of the classes in the past said, "Now wait a minute, Mr. Smith. What does multiple signal handling capacity mean? Does that mean this signal in this case and that signal in another case? Or does that mean two signals at the same time? What does it mean?" He said no. Why not? Why can't multiple signal handling also be simultaneous? Why can't it?

Comment: It doesn't matter. You classify it.

Mr. Smith: You can?

Comment: Yes.

Mr. Smith: But the point is there's another problem here. What's the problem? The guidance isn't sufficient. Isn't that right? That's what it means to me. The classification guidance isn't sufficient.

Comment: Also, it might not be the full capacity.

Mr. Smith: You've got me. I don't know. She said it may not be the full capacity. I agree with you on this. I really do. You know, we could get into some theoretical discussion now, and I'm lost in a second. First this gentleman.

Comment: This brings up an interesting point. What happens when you've got a system that has a threshold. You can handle ten tanks with this system.

Mr. Smith: Okay, we can stop ten tanks at one time.

Comment: You can stop ten tanks at one time with my system. However, I can publish nine.
It's UNCLASSIFIED. How do you handle that?

Mr. Smith: Now you're talking — wait a minute. Are we talking about multiple — are we talking about — what am I trying to say? Compilation of classified.

Comment: No, no. I've got a contractor. He likes to publish stuff and he wants to talk about this system that he's developing for me. He doesn't ever say that it will shoot down or handle ten tanks. But he says nine sometimes. He says eight sometimes. What do you do?

Mr. Smith: You look for some specific classification guidance in a case like that. I had a similar situation. This has to do with complications. I have the coordination of 500, or however many there are, of the missile silos in the United States. I don't know how many there are, ICBM silos. If I know all 500 of them, that's classified SECRET. But if I know one, that's UNCLASSIFIED. Or if I know number 23, that's UNCLASSIFIED. Now he says to me — let me just follow this up and then I'll let you — he said, "Suppose I had 499 of them, Mr. Smith? Is that still SECRET information?" "Oh," I said, "it's got to be. It's got to be." He said, "What about 498?". And it struck me then that — he said, "You know what's going to happen?" And you know what's going to happen. "I'm going to reach a point of no return. Sooner or later I'm going to have to make a decision."

Comment: There's a court decision in that.

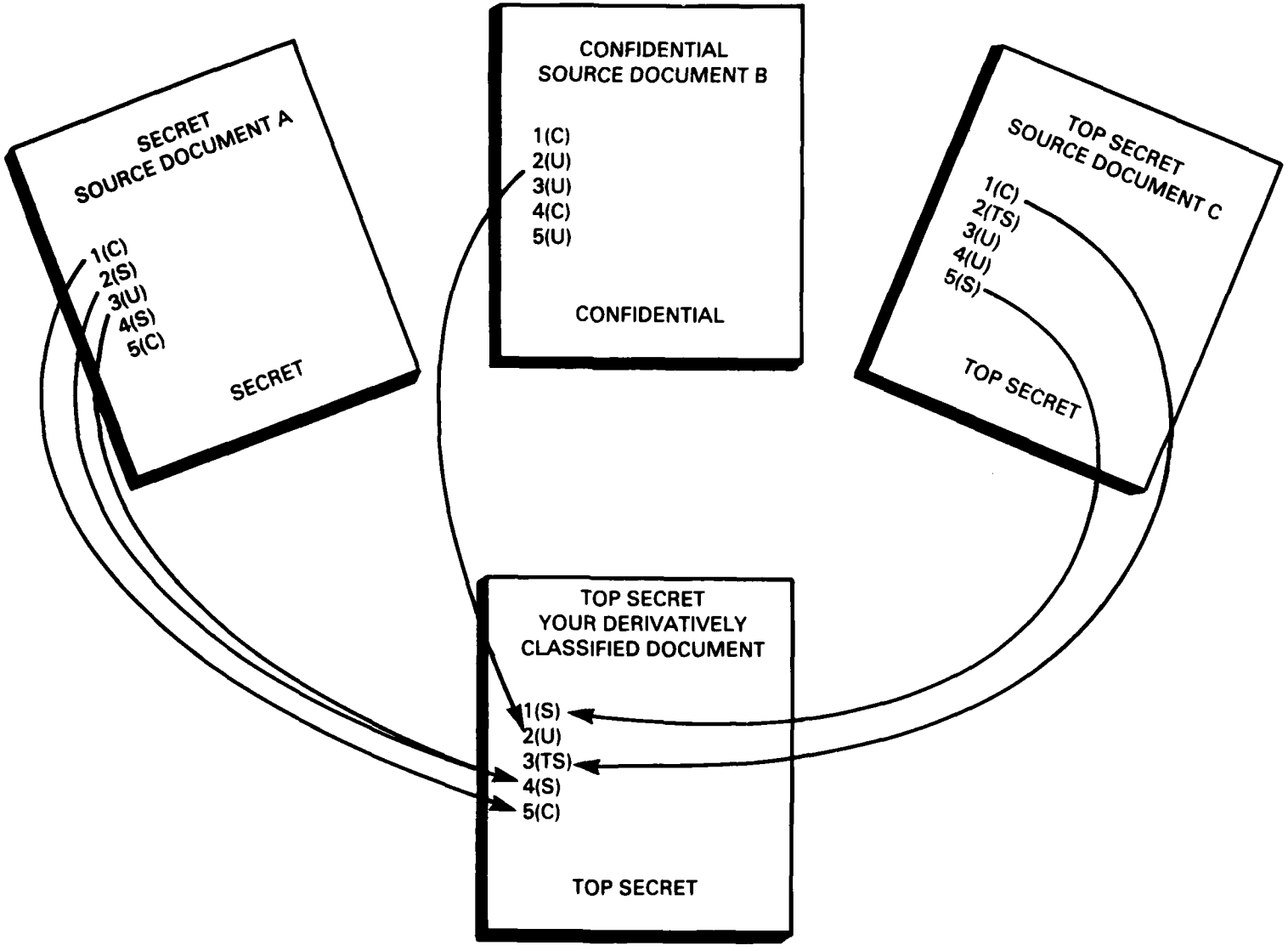
Mr. Smith: Oh, yes. I know what you're talking about. You're talking about our friend. Who he's talking about here? W.L. I think that's the one he's talking about and that happened five years ago. An article in the Washington Post said no secrets equate to big secrets.

Comment: In other words, the compilation is never released to every individual component.

Mr. Smith: Exactly right. Judge Green, if you'll recall, said, "I did not address the concept of compilation as classified information. I only ordered the DoD to release all unclassified portions of that document." So anyway, yes, it's a good question. I think that's essentially what you're talking about.

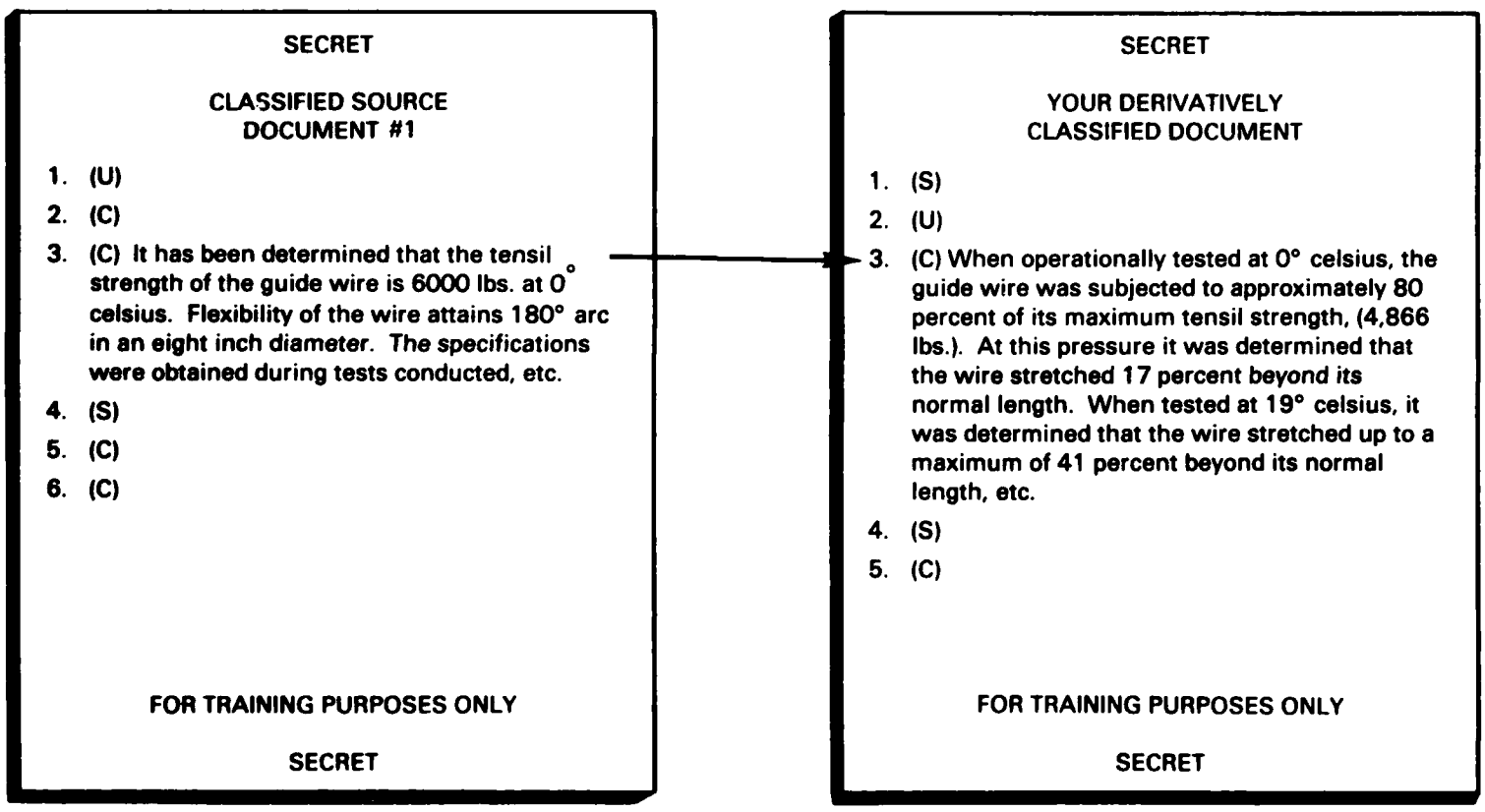
Comment: Two questions. He raised the second one. The first one dealt with the manner in which

APPLYING DERIVATIVE CLASSIFICATION
Utilizing Classified Source Documents



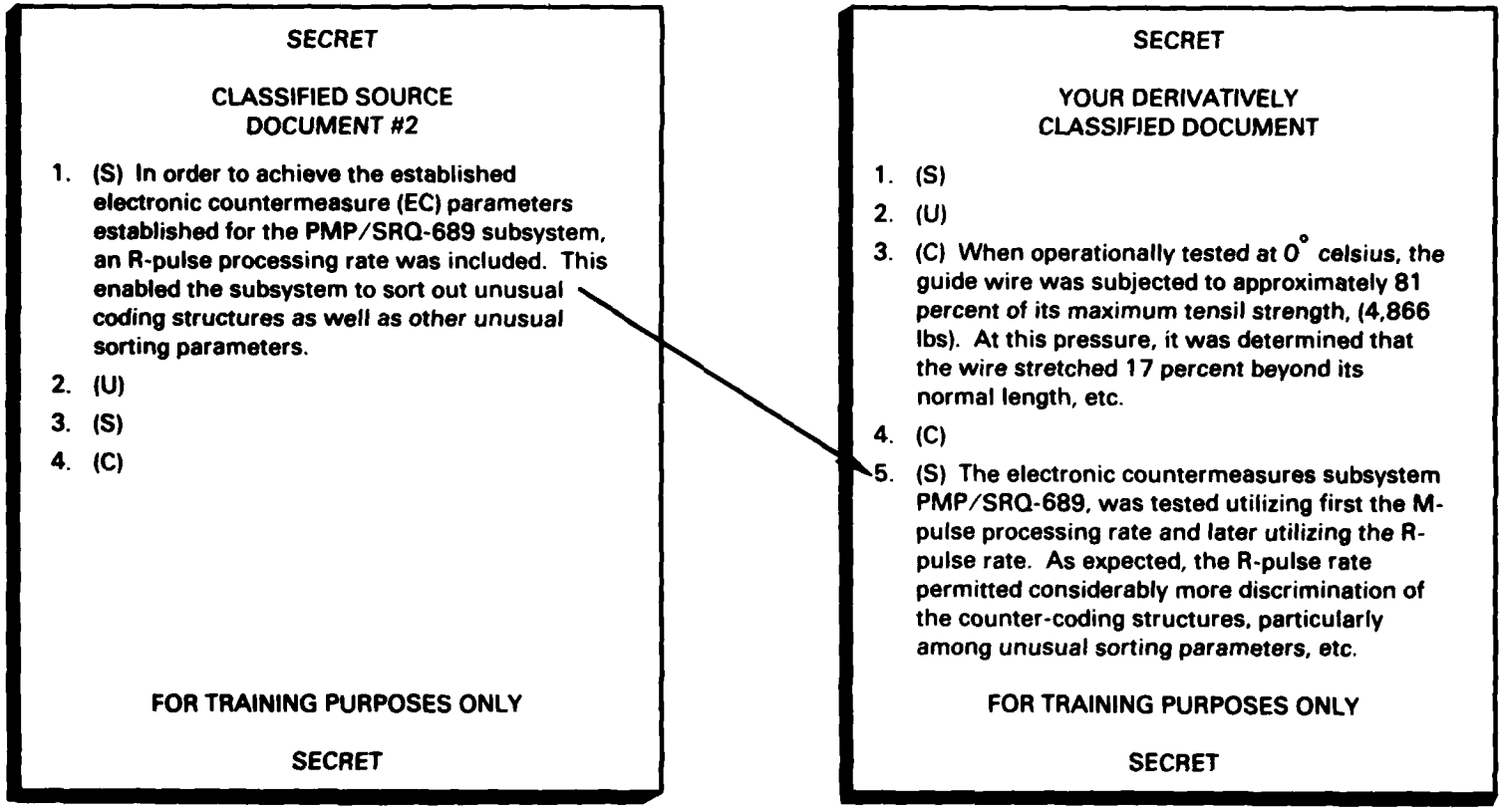
ENCLOSURE 1

APPLYING DERIVATIVE CLASSIFICATION



ENCLOSURE 2

APPLYING DERIVATIVE CLASSIFICATION



ENCLOSURE 3

SECURITY CLASSIFICATION GUIDE

X MAR 477 - MOD 3 - WIRE GUIDED TORPEDO
NAVAL SEA SYSTEMS COMMAND
WASHINGTON, D.C.

SECTION 3 SPECIFICATIONS FOR GUIDE WIRE

	CLASSIFICATION	DECLASS. DATE	REMARKS
A. TYPE	U	—	—
B. COMPOSITION	S	1 MAY 1990	—
C. CAPABILITY (COMMUNICATIONS)	U	—	—
D. FLEXIBILITY	C	1 MAY 1990	—
E. PLAYOUT SPEED	C	1 MAY 1990	—
F. WEIGHT (PER 100 MTRS)	C	1 MAY 1990	—
G. TENSIL STRENGTH	C	1 MAY 1990	—
H. ELASTICITY	C	1 MAY 1990	—

SECTION 10 TESTING PROGRAM

A. TEST PHILOSOPHY	U	—	—
B. TEST OBJECTIVES	U	—	—
C. TEST SCHEDULES	U	—	—
D. TEST DATA, ANALYSIS, AND CONCLUSIONS REVEALING CAPABILITY, LIMITATIONS, WEAKNESSES OR VULNERABILITIES OF THE GUIDE WIRE	C	1 MAY 1990	—

SECTION 12 VULNERABILITIES AND WEAKNESSES — SELF DEFENSE SUBSYSTEM

A. OVERALL PERFORMANCE	S	1 MAY 1990	THEORETICAL OR MEASURED DATA
B. PMP/SRQ-689			
a. SPECTRAL/FREQUENCY CHARACTERISTICS	S	1 MAY 1990	—
b. PERFORMANCE CHARACTERISTICS/ LIMITATIONS	S	1 MAY 1990	THEORETICAL OR MEASURED DATA
c. SYSTEM CAPACITY	S	1 MAY 1990	INFORMATION DISCLOSING MULTIPLE SIGNAL HANDLING CAPACITY AND OPERATING MODE DETAILS

you're going about questioning your source classification document, the guide itself. You're digging in. You're saying does that mean this, this, this, and this. You're playing devil's advocate.

Mr. Smith: Yes, I guess I am.

Comment: To what degree do you stop and say, "Hey, there's logic in what the man's trying to tell me. Am I going to address this or am I going to play devil's advocate with it until I get to a point where he doesn't even know what he's doing?"

Mr. Smith: Well, don't you think as a derivative classifier you have to get to the point where you're satisfied?

Comment: I'm asking you, is that what we have to do? You're doing the instructing. All I'm saying is tell me I have to.

Mr. Smith: Yes, that's what you have to do.

Comment: That's enough.

Mr. Smith: You have to satisfy yourself that you understand what each classification means. How at times that might mean referring back to the original office of original classification saying, "I need further clarification on this." Another thing you'll see. Most classification guides say this, "We invite you if you can come up with any suggestions or ideas to improve the classification, the clarity, whatever it is, whatever aspect of that classification guide, we invite you to assist us in doing that." So I think that's part of our responsibility as a derivative classifier. But the problem it seems to me is that most people go along blithely doing their thing, so to speak, not recognizing that what they're doing is giving no thought to at all. And as a result, we get this total inconsistency in classification. And that's the least that can happen. In some cases it would result in the compromise of very sensitive classifier information. Yes, sir.

Comment: Most security classification guides list a point of contact, usually with a telephone number where at least you can call that organization that put it out.

Mr. Smith: Exactly right, exactly right. Although what is your first obligation? You've got the guide.

You're going to try to get everything you can out of the guide, aren't you?

Comment: Certainly.

Mr. Smith: Sure, but if you're not satisfied, it will eat at you. You know what I mean. I'm trying to get emotional about this thing, but that's the fact. So each person I think has to make that decision for himself. Have I gone as far as I can? Am I satisfied? If I'm not, I'd better try to do more. So that's the only way I can answer it because we're talking about something very subjective.

PANEL PRESENTATION ON INTERNATIONAL PROGRAMS SECURITY REQUIREMENTS, INCLUDING PROBLEMS OF UNITED STATES, CANADIAN, AND UNITED KINGDOM CONTRACTORS

James J. Bagley (Moderator)
R&B Associates, U.S.
(Past NCMS President)

Robert T. Grogan
Department of Supply and Services
Ministry of Defence, Canada

Edgar G. Hill
Director of Security
Ministry of Defence (Procurement Executive), U.K.

Arthur F. Van Cook
Director of Information Security
Office of the Under Secretary of Defense (Policy), U.S.

John McMichael, M.B.E.
Chairman of the Guild of Security Controllers, U.K.

James E. Wyatt
Director of Business Operations
Marconi Electronics Corporation, U.S.

Robert J. White
Director of Security and Safety
Cincinnati Electronics Incorporated, U.S.

Mr. James J. Bagley: This panel was actually conceived about 1979, shortly after the then Under Secretary of Defense Perry wrote a couple of memoranda on international cooperation. The memoranda at that time raised a few ripples but didn't get much attention. There was a general feeling in some quarters that the subject would go away, but it didn't. Shortly thereafter an article appeared in the 1979 Journal commenting on those memoranda and highlighting some of the problems that were not addressed at that time. The article was not very sanguine about the future of the program.

The Industrial Security Manual (ISM) and Industrial Security Regulation (ISR) have been Modified to implement the industrial security agreements concluded by the United States (U.S.) with Canada and with the United Kingdom (U.K.) by which reciprocal clearances could be granted to Canadian or U.K. firms under the Defense Industrial Security Program. In 1982, the Federal Republic of Germany (F.R.G.), was added to that particular reciprocal clearance program. Other countries have been involved and will be included.

NCMS has had numerous panels and presentations on international programs over the years. Principally, those subjects concerned the U.S. doing business overseas and discussed such problems as the international traffic in arms regulations, export control problems, the problems of joint ventures, and now and often the currently popular subject known as technology transfer.

The subject of U.S. firms, foreign-owned, doing business in the United States with the Department of Defense has not been discussed. As far as I know, this is the first panel held on this subject by a major society where the principal players, government and industry, are present.

The panel consists of two parts, but it has a single purpose: to inform and educate you on the problems, policies, procedures and implementations of them that is taking place right now.

The reciprocal clearance process is new, but from direct observation I have drawn a few personel conclusions: that there is an obvious lack of communication on the government side between the operational planners and their acquisition counterparts, between, acquisition and procurement, and between procurement and security. This condition exists within and between the military departments. It is apparent, therefore, that much education, much learning, much trial and error must take place. So that is our purpose.

Putting together this panel has been a labor of love because I am convinced that there is a genuine feeling of wanting to get the job done on the part of the individual governments involved. They wish to make the process work to remove the hassles that are inevitable so that this program can be viable. In industry there is always and has been a feeling of frustration because the problem is new and the policies and implementing procedures have not been fully developed. There, too, is a feeling of wanting to get the job done within existent policies with a minimum amount of red tape. The program is in place and I think we are all trying to make it work.

The government panelists here are all members of NCMS. Mr. Robert T. Grogan from the Ministry of Defence in Canada, Mr. Edgar G. Hill from the Ministry of Defence, U.K., and Mr. Arthur F. Van Cook from the DoD, U.S. The industry panelists are Mr. John McMichael from the Guild of Security Controllers of the U.K., Mr. James E. Wyatt from Marconi Electronics, and Mr. Robert J. White from the Cincinnati Electronics Corporation.

To avoid the obvious protocal problems, I will present the government representatives in alphabetical order. First, it is my pleasure to introduce Mr. Robert T. Grogan from Canada.

Robert T. Grogan: Let me say at the outset how pleased I am to be here and have the opportunity to participate in this panel dealing with international programs and problems arising from the security requirements applicable to such programs. In the time available for this formal presentation, I would like to comment on the background to the Cana-

dian international program arrangement with particular focus on Canada-United States situations. Then I'll deal with certain security problem areas from our perspective.

While Canada maintains bilateral defense production relationships with a number of countries — and those countries are mostly within the membership of the NATO alliance — there's no question that the major relationship and the one that impacts most significantly on our defense industries and which has reciprocal features, which Mr. James Bagley just mentioned, is the one with the United States. The United States and Canada maintain close political and integrated military cooperation on the North American defense system. Both governments accept the coordination of economic efforts in support of their common defense. As a matter of policy, Canada shares the cost of North American defense with the United States (not on a one-to-one basis naturally) and procures much of its defense material and other requirements from U.S. firms. For example, the CP-140 Aurora, a long-range patrol aircraft, was procured from Lockheed in California. The CF-18 Hornet aircraft, which is our replacement aircraft after 20 some years of the 104 Starfighter, the contract has been awarded to McDonnell-Douglas, the single biggest defense contract ever awarded in Canada at the time.

A cooperative program bilaterally approved in 1960, and titled the United States — Canada Defense Production Sharing Program, was designed to assure Canada a fair opportunity to share in the development and production of U.S. weapons and equipments. This would help to sustain the defense technological and productive resources of Canada at essential levels and contribute directly to the U.S. defense industrial base in North America. Joint R&D collaboration and defense production and development sharing programs are also in place which enhance industrial preparedness and planning. A significant mechanism in the context is the Canadian Commercial Corporation, a Federal Crown Company, as we title it, which is through an agreement negotiated with the Department of Defense solely responsible for the management of Canadian industrial participation in that particular planning and programming system.

The foregoing defense related programs give rise to many security requirements which could be broadly covered in the United States — Canada general security agreement. However, it is the bilateral United States — Canada Industrial Security Agreement of 1952 (30 years ago) and its related operating procedures, which were updated in 1971 at ministerial level, that really provides the working mechanism for our cross-border transmission of classified information and material, reciprocal personnel and facility security clearances, document safeguarding standards and classifications, and visit clearance arrangements.

Within the security framework of ongoing international program activity, there are bound to be problems from time to time. I am pleased to report that they are few and infrequent from our standpoint today. But from what I learned here probably not that simple for the future. Nonetheless, frustration and sometimes disappointment and anger arise for our private sector associates when they bump up against delay imposed by security requirements affecting their marketing and their contractual initiatives.

Recently we had a situation where a Canadian corporation which had no prior need for a facility security clearance in Canada bought control of a U.S. company which had and did. There was initially a reluctance on the part of the Canadian parent and its key officials to go through the personnel security clearance process because it meant that their officials would have to submit to the personnel security clearance requirements that they had never done before. Fortunately, gentle persuasion and explanations by our field officer brought them into line, but it was a reciprocal facility assurance issue which gave rise to the initial problem.

My staff working with and through the Defense Investigative Service (DIS) has not had any insurmountable difficulty in arranging mutually acceptable transmittal channels for classified documents and materials. Problems arise sometimes when our respective postal authorities change weight limits and such on long established and accepted systems, such as registered mail. Our post office did so last January and completely

pulled the rug out from under us by limiting that class of mail to 500 grams or approximately one pound. Consequently bulk document shipments have to be routed through other arrangements, sometimes less expeditious, in order to meet at least an equivalent standard of protection to that afforded formerly by our registered mail system.

Visit clearance lead-time is the most prevalent and vexatious problem we're contronted with. The 30-day lead time demanded by DoD translates into 45 days at our branch headquarters level in Canada. Compounded, of course, is the lead time with Canada to get it from industries in Canada to us. Notwithstanding that, we recieve much assistance from DoD through our Washington Industrial Security Liaison Office at the Canadian Embassy.

In really urgent cases binationally we're faced with a proximity to one another over the longest unguarded border in the world, and we have airline service that takes you from a city in Canada to another in the United States in jig time. That together with telephone, telex, facsimile, et ecetra, has our clients in Canadian industry frothing at the mouth and complaining regularly about what appears to be an inordinate delay and lead time for them to make personal contact on potential or actual contracting activities with their colleagues in U.S. defense industries.

We offer a five-day lead time in a reverse situation. However, our companies are fewer. We only have at the most at any given time about 400. I do not have to contend with military command channels in processing visits to our companies, because I work for the Department of Supply and Services. I work for our National Defense Department, but the program is controlled within our department, and I don't have to work the command channel.

Mr. Bagley: And now it is a distinct pleasure to introduce to you another NCMS member, Edgar G. Hill, from the United Kingdom, Ministry of Defence.

Edgar Hill: My task is to describe in ten minutes the security arrangements which the Ministry of Defence (MOD) applies when it or one of its contractors places United Kingdom classified work with a U.K. firm which is foreign-owned, controlled, or influenced to a significant extent or with a foreign firm located in a foreign country. It is one of the quirks of our Parliament that any member may introduce legislation on any subject, controversial or otherwise, under what is known as the ten-minute rule. And one of the benefits of that rule is he knows he's not going to be interrupted. For the purposes of my talk this morning, I'm regarding classified work as work involving TOP SECRET, SECRET, and CONFIDENTIAL. As you've heard, we still have the RESTRICTED grading, and under that a contractor only has to take elementary precautions. I will also concentrate on the situation where the ownership or the firm itself is located in the United States, with whom we have a comprehensive industrial security agreement. The position with other friendly countries vary, and as Mr. Robert Grogan knows, we have unwritten understandings with Canada.

At the outset, I must stress that United Kingdom's practices and procedures tend to be far less formalized than your own, but I believe no less effective. There are benefits in not having a written constitution.

In the United Kingdom there's no equivalent of a U.S. contractor entering into a security agreement with the DoD on Form DD 441. A firm in the U.K., whether U.K. or foreign-owned, does not have to seek a formal facility security clearance before it may be considered for U.K. classified work. In placing or permitting one of its defense contractors to place classified work for the first time with a firm located in the U.K. and owned by an interest in a friendly foreign country, the Ministry of Defence first seeks confirmation from the other government that the foreign owners or themselves are acceptable from a security point of view. Usually, of course, they're found to be in the same line of business and performing similar work for their own national government. If the firm is American, then confirmation is sought through the industrial security arrangements.

Assuming everything is satisfactory, the further security criteria and arrangements applied by the ministry are substantially the same as they would be if the firm were completely U.K.-owned. A

person of undoubted reliability is selected as the initial security contact with the firm. We can then proceed as necessary with the requirement under our standard conditions of government contract, that if and when directed by the authority, the contractor shall furnish full particulars of all persons who are at any time concerned with any SECRET matter. I'm not aware, incidentally, that a U.S. firm has ever taken over a U.K. firm and then decided to staff it entirely with U.S. nationals.

Standard Condition 59, as it's called, and its subcontract equivalent are specific in requiring the exclusion of aliens and naturalized British subjects from classified work. But the Defense Secretary has authority to waive this exclusion when it is in the MOD's interest to do so. In fact, most of those come to me for a recommendation, and it's quite interesting sometimes to see how central a particular typist is claimed to be. I had one the other day and the case was put direct to me rather than through my staff because they thought that I ought to know that the particular lady had a contact at a very high level. When I took the precaution of going to that level, he said that he had never heard of the dear lady in his life.

But such a waiver could be granted to a U.S. citizen who is acceptable from the U.S. authorities from a security point of view and who is appointed to a U.K. firm being taken over by a U.S. firm.

Negotiations and tendering commence; and if successful, a classified contract or a subcontract is placed with the firm. This contains a security clause under the standard conditions if the work is placed by the ministry direct, or another form, if placed by one of the ministry's contractors. Both spell out the firm's responsibility to protect any classified information and gives the ministry or the ministry's contractor the right to exclude persons from the work without giving a reason and to terminate the contract if the firm is found to be careless or incompetent in its security practices.

For its part, the ministry must define the classified contract in writing. After the contract is placed, the firm is supplied with detailed security instructions and procedures, is given on the spot security advice, and receives assistance in bringing its facilities up to an acceptable security standard. All this, of course, is very similar to your own arrangements; but there are some significant differences.

The U.K. has no formal equivalent of the provision in the U.S. regulations which prohibits certain important types of classified information from being released to U.S. firms in America which are under foreign ownership, control, and influence. There may be some information to which access is limited, but we do not as a matter of principle formally prevent approved U.K. nationals working in U.S.-owned firms in the U.K. from having access. The foreign ownership of the firm is not itself regarded as a security objection to the placing of work involving access to U.K. classified information.

As examples, the U.K. subsidiaries of Sperry and RCA are employed (I now have to say were employed, in the case of Sperry, because Sperry's have now been retaken by a British firm) upon U.K. government work of the highest confidentiality. This includes what you would term Restricted Data. Arrangements broadly similar to those I have outlined apply when a U.K. firm already performing classified ministry work is taken over by a foreign interest. I should add that the need-to-know principle applies,and if there's one thing I've learned in my four and a half years, it's the importance of the need-to-know principle.

I had a case the other day when a very senior military chap left the MOD and set up his own firm. And then he asked to be supplied with all our draft targets and requirements so that he could be kept in touch in the future. You can guess what answer he got — polite of course.

In the need-to-know principle, we do not, for example, grant clearance to board members simply because of their status. Visitors from the parent company would only be given access if this was essential for the performance of the contract. Any such information would need to be cleared with MOD and transmitted through government to government channels. To do otherwise would be a serious default of contract.

When U.K. classified work is to be placed with a foreign firm located abroad, the considerations

are similar. As well as obtaining an assurance about the security acceptability of the foreign firm, the U.K. obtains from the other government confirmation of the firm's capacity to handle and protect the classified work and information. If all this is satisfactory, a contract is placed containing an appropriate security clause. If the firm is in the United States, the form of the clause has been agreed with the appropriate national security authority. Generally such clauses require the foreign contractor or subcontractor to restrict access to classified information to persons authorized for access to the foreign country's own equivalent information. Thereafter, security provisions and supervision are provided by the other government. Again, there are no formal restrictions upon the type of work that may be placed abroad.

Documents classified CONFIDENTIAL or above are usually passed through the firm through diplomatic channels by a government-to-government transfer, but occasionally there are special arrangements for a personal carriage of documents when urgency is paramount. These special arrangements are in line with the NATO regulations for the transmission of documents classified NATO CONFIDENTIAL or SECRET. However, I understand that at present your regulations do not permit a U.S. contractor's employees to transport classified documents across international borders.

Another difference concerns the U.K. attitude toward the authorization of international visits to firms where our advance notification requirements are less stringent. We, in fact, had one vice president of a company who turned up at the gate at mid-day completely unannounced. I'm happy to say that he was let in after a few phone calls.

I'm occasionally asked about how U.S. firms should set about obtaining a U.K. classified defense contract or subcontract. If the work is to be placed directly by the ministry, and not by a contractor to the ministry, a U.S. firm operating in the U.S. or a U.K. subsidiary applies to be considered in the ministry's trade list of contractors for the type of work. No firm, U.K. or foreign, has a right of inclusion on these lists. Firms are listed if further capacity is needed for the type of work or if a possible requirement is foreseen for their services. Firms may also inform relevant Ministry of Defense project authorities and R&D establishments of their capabilities. Firms operating in the U.S. may also inform the U.K. Defense Procurement Office at the British Embassy in Washington of what they can offer. But this is on an information-only basis initially. It's rather like the theatrical agency — don't call us; we'll call you.

Subject to security considerations, the ministry's main contractors in the U.K. are generally given a free hand in subcontracting. A U.S. firm hoping to obtain a subcontract should make their services known to the main U.K. defense contractors.

There are no formal arrangements for informing firms, U.K. or foreign, of opportunities for classified or unclassified U.K. defense work. Contracts and tenderings are not formally advertised as is the case in some other countries. Firms, whether in the U.S. or U.K., need not be restrained from indicating an interest in classified work merely because they are not at present authorized to perform work of equivalent classification. If the ministry has the need to invite tenders, it will initiate the necessary security procedures.

Finally, I would like to say a few words about multinational industrial consortia. With the increasing standardization of equipment throughout NATO, it is now not uncommon for a company to be set up which is owned equally by a number of parent companies in different countries. An example UKAGE Systems Limited which was formed to bid for the U.K. Air Defense Ground Environment System and it won. The company is registered in London, but is jointly owned by the two British companies, Marconi and Plessey, and the Hughes Aircraft Company. Work is carried out by the three parent companies on their own locations in both U.K. and the U.S. and also at the London office which is manned by personnel from each country who have been secured for the duration of the contract.

The U.K. places little restriction on the information which is passed to UKAGE Systems Limited or the U.S. staff in UKAGE Systems Limited who have appropriate U.S. security clearances. Of course, when various parts of the work are performed in another country, there are inescapable problems. Instead of an engineer popping down the corridor to see his colleagues, he must in conformity with

security regulations, both U.K. and U.S., suffer the inherent delays incurred by international visit clearance and government-to-government exchange of information. These delays may have potential serious repercussions particularly when deadlines have to be met.

On the current Multiple Launch Rocket System (MLRS) which is still at the competitive stage, six consortia have been formed and each consists of a firm in France, West Germany, U.K. and U.S. You'll see that our problems are not multiplying. However, the four governments have cooperated and special arrangements have been agreed upon that will facilitate exchanges of information between the partners of each consortia. These arrangements allow contractors' representatives to act as couriers for the international carriage of classified documents. We hope this concession will also apply to employees of the involved U.S. companies. There are clearly problems in this collaborative effort that need to be addressed very quickly if things are going to run smoothly in the future.

One of our nobility said some years ago, "Don't go abroard. It's a beastly place." Sorry, "It's a dreadful place." Let's hope no one said, "Don't collaborate. It's a dreadful business."

Just before I left the Government published a statement on the recommendations of a security commission which has been looking at the U.K. security procedures and practices. I would like to read the paragraph dealing with classification because it is germane to these discussions. The commission has said on classification as follows:

"The aim of both physical and personnel security is to prevent the disclosure of information acquired by public servants in the course of their official duties to anyone who is likely to use it to the injury of this country. The methods used are, on the one hand, physical protection and on the other denial of access to classified information by persons whose loyalty and reliability have not been confirmed by previous investigation. The degree of protection depends on the security classification accorded to the information in question. The system of classification thus lies at the root of security procedures in the public service.

"In the commission's view overclassification is the error that is most commonly committed in carrying out current security procedures. This is not only objectionable on grounds of managerial efficiency and economy, it adds considerably to the expense of security procedures and the manpower needed to carry them out. Even more important, it is liable to undermine the effectiveness of the procedures themselves.

The commission therefore recommends that there should be a thorough review of the classification system designed both to limit the number of newly created papers with a high security classification and to attempt to bring about early reduction in the classification of papers once they have been created. More gfenerally, the commission recommends that the manuals providing security guidance to departments should be revised so as to make the instructions they contain clearer and easier to consult."

What I have learned from this Society over the last three years will be of considerable benefit in that review.

Mr. Bagley: And last but no means least, a dear friend and colleague, Arthur F. Van Cook.

Arthur F. Van Cook: I'd like to comment on the bilateral security agreements mentioned by my colleagues from the United Kingdom and Canada and explain their effect on U.S. firms under foreign ownership, control and influence (FOCI) and touch briefly on our visit procedures.

In previous presentations to this group, I have indicated that one of the criteria which must be satisfied, prior to releasing U.S. classified military information to foreign governments, is whether the recipient government has the intent to protect the information as we, in the United States, want it protected. Now this intent is established by the negotiation of a bilateral security agreement with the foreign governments of our interest.

First there is the general security of information agreement that is negotiated through diplomatic channels on a Department of State-Ministry of Foreign Affairs basis. We have 43 such agreements either in place, being updated, or action has been initiated to put them in place. This agreement states that each party to the agreement will afford,

to classified information provided by the other, the degree of security protection afforded to it by the releasing government. It contains provisions concerning the use of each other's information, third party transfers, and private rights. It stipulates that both parties will agree to report any compromise or possible compromise of classified information provided by the other party, and further that an investigation will be conducted of each occurrances, and the results of the investigation along with the corrective action taken to preclude recurrence will be provided to the originating government. It states that both parties agree to permit visits to their territory by security experts of the other to review their security laws, procedures, and practices for the purpose of ascertaining their capability to adequately provide the requisite degree of security classification protecting of classified information. We have had this exchange of visits between governments represented here and have been quite satisfied with each other's ways of protecting our information.

Now the General Security of Information Agreement (GSOIC) provides that classified information will be exchanged on a government-to-government basis. The Industrial Security Agreement is an annex to the GSOIA. We put those in place with those governments with which the DoD has established co-production, co-development, and/or reciprocal procurement arrangements involving industrial industry participation. We expect that there will be 18 or 20 of these Industrial Security Agreements in place very shortly.

The Industrial Security Agreement includes provisions for clearance of facilities and personnel, the handling and transmission of classified material, and procedures for visits. It specifies security clauses to be included in classified contracts and identifies the government agencies responsible for industrial security matters. In our case, of course, that particular agency is the Defense Investigative Service (DIS).

Like the GSOIA, the Industrial Security Agreement requires that classified information be exchanged through government channels. As my Canadian and United Kingdom colleagues noted, certain Industrial Security Agreements contain a reciprocal clearance provision. It's an appendix to the annex. Of the 18 or 20 Industrial Security Agreements that the United States, will have in place with other governments, very few of these will have that reciprocal clearance provision in the agreement. We do have them with the United Kingdom and with Canada. This permits either signatory government to clear one of their firms which is under the FOCI of the other government.

Before I proceed with my discussion of reciprocally cleared firms, let me explain what we mean by foreign ownership, control, or influence, or FOCI. It's fairly common for U.S. defense contractors, certainly the larger and more deversified ones, to have some degree of foreign involvement. When the nature and extent of FOCI is such that a reasonable basis exists for concluding that certain classified information released to the firm or the foreign government represented may be made accessible to the foreign parent firm or the government effected, the effected contractor is considered to be under FOCI. As such, it would be ineligible for access to classified information under DoD procedures and a facility security clearance would not be granted, or it would be subject to revocation as appropriate.

When there is a significant degree of FOCI —for example, if the amount of stock owned by the foreign interests is sufficient to permit representation on the U.S. firm's board of directors — a voting trust or proxy agreement is a means of insulating the U.S. firm from foreign interest. In order for such arrangement to be approved, the foreign owner must agree to relinquish all the normal perogatives of management. When a contractor establishes such a trust or arrangement, it is generally possible for the U.S. to issue or continue the facility security clearance; and the firm is no longer considered under FOCI. It may have access to U.S. classified information and be awarded classified contracts just as any other U.S. firm.

However, in certain cases the parent firm for various reasons may not want to establish a voting trust or proxy arrangement. In such case, the only way the U.S. firm under FOCI may be cleared is through the reciprocal clearance arrangement, if the Industrial Security Agreement with the foreign government involved contains such provisions.

Under the terms of the reciprocal clearance appendix, a U.S. firm in the United States under the FOCI of a foreign interest might be eligible for a reciprocal facility security clearance based on the assurance of the foreign government that the parent firm (parent foreign firm) has a facility clearance at the appropriate level. A citizen of the foreign government working at the U.S. firm would also be granted a reciprocal clearance based on the security assurance provided by the parent or the government represented.

However, as in the case with the granting of any facility clearance, a U.S. contracting agency must sponsor the action pursuant to the performance on a classified contract. This procedure works in the reverse order for a foreign firm under the ownership, control, or influence of U.S. interests. In most aspects a U.S. firm with a reciprocal clearance is treated like any other U.S. firm. However, there are two important differences.

First, the granting of a reciprocal clearance to a U.S. firm under these procedures does not remove it from FOCI as is the case with a voting trust or proxy arrangement. Consequently, before the U.S. firm may have access to U.S. classified information, a determination must be made that the information is releasable — not released but releasable — to the foreign government represented. That determination is made under our national disclosure policy guidelines. This determination, releasability of the information to the foreign government, must be made whether the information to be released is in documentary form or oral pursuant to a visit. Further, a U.S. firm under FOCI is a representative of a foreign interest as defined in the DoD ISM even though it has a reciprocal clearance.

As I stated earlier, the GSOIAs and Industrial Security Agreements require that classified information be transferred through government-to-government channels. Therefore, classified information to be released to a reciprocally-cleared firm must be transmitted through government channels under our procedures. To do otherwise, in our view, would be a violation of our bilateral security agreements with the other government.

Before closing, I'd like to say a few words about our visit procedures since this matter was raised by Mr. Robert Grogan. The DoD policies concerning the release of classified military information to foreign governments and international organizations are based on law, Executive Orders, and Presidential Directives. These issuances prescribe rules for the protection of U.S. classified material and require that such material be released on a government-to-government basis. Further, care must be exercised to assure compliance with U.S. government arms export laws as set forth in the State Department's International Traffic in Arms Regulation (ITAR).

In this connection, government arrangements for visits cannot be used as a means to bypass the provisions of the International Traffic in Arms Regulation. Government arrangements must be in support of a government-to-government program such as a reciprocal procurement Memorandum of Understanding (MOU) or data exhange agreement. For these reasons, DoD policies differentiate between access to U.S. information in technology by foreign government officials and access by representatives of foreign industry, and between contacts by foreign representatives with DoD officials and contacts with U.S. defense contractors.

As I discussed earlier, the GSOIA and industrial security annexes specify certain procedures and channels for exchanging classified material that are binding on both parties. In addition to the legal and policy considerations, DoD visit procedures are influenced by the sheer magnitude of foreign requests for visits and information and the necessary coordination required for such visits.

Mr. Robert Grogan mentioned that he did not have to work with the military departments and agencies as we do. He also mentioned that in his country they have about 400 firms. In our case, I think Mr. Thomas O'Brien mentioned that we have about 11,500 cleared facilities; and we do have to work with the military departments and defense agencies. The DoD officials receive in excess of 45,000 requests for foreign visits each year and each request averages seven visitors, and many of them involve visits to more than one location. The same foreign liaison staffs that process visit requests also process foreign government requests for U.S. documentary information. The services receive

approximately 8,000 of such requests annually, ranging anywhere from one to over a hundred documents involved in each request.

Under our national disclosure policy, disclosure decisions rests with the originator of the information. The foreign liaison staffs in the military departments and the Defense Intelligence Agency do not make the decision to approve a visit or a document request. The originator of the information involved must make that decision. In some cases where the information proposed for disclosure is of interest to another department or agency, the request must be coordinated with that element. If a visit request is received which entails visits to several DoD elements and defense contractors and a different subject is to be discussed at each, the coordination of such a request, as you can well imagine, takes time to process.

To overcome delays in obtaining visit approval, we've established what we call extended visits. Under this procedure, a foreign government may request a blanket visit authorization to permit recurring visits for up to one year. Any number of foreign government or industry personnel may be listed on the request, and the request may involve visits to several U.S. government or contractor facilities. However, the request must be related to a specific program project, or body of classified information. Once approved, the visitors may make direct arrangements with the U.S. facility to be visited on 72-hours' notice. Names of personnel on that type of visit authorization or locations to be visited may be changed on 72-hours' notice.

I have on numerous occasions encouraged our friends and allies with whom we have established reciprocal procurement MOUs or similar arrangements to make full use of this procedure. It has worked well in many cases.

I hope I've given you some further insight into what drives our procedures. And they are basically the agreements which are negotiated between the governments at the ministerial level.

Mr. Bagley: We have heard the government's side. Now we will take a look at the other side. Those of you who have spent a long time in government and have moved to the other world recognize very quickly the differences. Mr. John McMichael, chairman of the Guild of Security Controllers for the United Kingdom, will discuss first the side of industry.

John S. McMichael: I'd like to take this opportunity of sending greetings to you from the members of the Guild of Security Controllers. There is great interest in what's going on in the security world in the United States, and in particular, what you discuss here at the NCMS.

I'd also like to say how nice it is — and I'm sure I'm speaking on behalf of my other international colleagues — to see that our National flags are represented here at this meeting. We've got a particular interest in restoring ours in a certain part of the universe.

My talk will deal with international collaborative projects. First, I should explain that I will be mentioning the term "security controller" throughout my talk, and that term is the official designation by which we are known.. You may be a manager, a security director, a chief security officer, but in official parlance we call ourselves security controllers. I am presenting this paper on behalf of the Guild of Security Controllers whose members are very much at the sharp end of industrial defense security business. It is on their shoulders that the burden of the many and various security procedures fall.

As time is limited, I will only deal with a selected number of security procedures concerning international collaborative projects.

A security controller in the U.K., whether he is employed on full-time or part-time security duties with a large or a small firm, is responsible for every aspect of industrial defense security as it affects a defense contractor undertaking one or many classified government contracts. In larger firms the security controller will have supporting staff to deal with such matters as document security and visits. His security manual is prepared and issued jointly by the Minister of Defence and the Security Service and lays down the minimum standards of security to be applied to any given situation relative to personnel, documents, physical, computer, and many other related security matters.

Our security instructions in our security manual

allow flexibility in interpretation in order to handle the many variations that we find in the defense industry. To supplement the security manual, various instructions are issued by the security authorities covering specific topics such as visit procedures and the handling and transmission of classified documents.

In the field of international collaborative projects, there are many difficulties in international cooperation. Defense security does not present more than a basic problem provided the participant countries are able to accept and rely on their respective partners' national security arrangements, particularly if they all happen to be member states of NATO.

In practice, security controllers come up against a number of problems when trying to implement standard security procedures concerning international visits, transmission of classified documents, and Telex and facsimile communications. These areas of concern are well known to the Government security policymakers who are taking steps to review policies and procedures.

First, I'd like to consider visits. In the U.K. the defense industry has to allow nine weeks for a normal visit request to be processed and approval has to be sought from respective U.K. project authorities to disclose the information in question which again adds many more weeks to the original nine. This applies equally to international collaborative projects or any other visit requirement involving the release of classified information, and despite the fact that an international collaborative project will be subject to the security agreement for industrial operations between the Ministry of Defence in the U.K. and the Department of Defense in the U.S. together with a Memorandum of Understanding which will be agreed upon before the outset of the collaborative project.

The Multiple Launch Rocket System III (MLRS) is a current international collaborative project involving the United States, West Germany, France, and the United Kingdom. This project has reached Phase III which has a time scale of six months to completion, proposals in the meantime have to be translated into French, German, and English. In this situation, time is of the essence at this stage of the project and a firm cannot afford to wait nine weeks for a visit request to be processed.

It is argued that participant firms should submit block clearances to cover up to a period of 12 months, assuring that all staff likely to be engaged on the project are included. But with the best of intentions, no guarantee can be given that all potential project staff will have been included. Staff members change jobs, and those with particular expertise are unexpectedly required to participate immediately and not a few weeks later.

Rules relating to visits stipulate that additional topics or establishments to be visited cannot be added to the original visit request. Names of additional staff can be added. This means that the overseas visitor who in the interests of a project is required to access new classified information or visit different establishments has to go through the whole procedure starting from square one.

Put yourself in the shoes of a security controller who must deal with a frustrated engineer when the security situation does not seem to make sense. Security controllers believe there needs to be more flexibility in visit procedures, particularly when international collaborative projects are concerned. Flexibility in visit procedures will lighten the load placed on the authorities who handle visits. The U.K., I believe, places the largest load on the U.S. system. Special rules could apply and the Memorandum of Understanding could provide for such rules to be introduced with the agreement of the participants. In such a situation the respective firms and/or establishments are known, and the national disclosure policy committees have approved the release of the classified information concerned. In such instances, visit requests could be clearly identified and certified by respective government visit authorities, such as DISCO and the International Visits Control Office of the Ministry of Defence (Procurement Executive), MOD(PE) as being associated with a specific international collaborative project. This would speed up the visit procedure and avoid the usual delays for formal clearance by the various departments.

Safeguards already exist whereby a visitor's access to a large extent is governed by the host contractor who is required to insure that the visit is

limited to those establishments and the classified information that has been duly authorized by the respective agencies. In the U.K. if a foreign visitor is required to access establishments and/or information beyond the scope of the original visit request, the U.K. contractor can apply to the MOD(PE) visit authorities for an extension of access without having to start all over at the visitor's firm or establishment. This situation is most welcome to both security controllers and visitors.

An equally important aspect of security is the question of transmission of classified documents between participant firms on a government-to-government basis. In the past a classified document could take up to eight weeks or more to reach its destination. On an international collaborative project with a tight time limit such delays are unacceptable. As with visits, the exchange of relevant classified or unclassified information has been identified and approved by the respective national disclosure policy committee. Therefore, the requirement to undertake the formal clearance procedures could be eliminated if adequate safeguards are built into the procedure to insure that where necessary the authorities are kept informed of the transmission between firms.

In order to meet deadlines, U.K. security controllers with MOD(PE) agreement are permitted to authorize staff to act as official couriers to hand-carry classified documents across national boarders. For MLRS III, a special dispensation has been agreed upon to permit the hand-carrying of classified project documents between participating firms with the proviso that in the United States the documents are handed over to the nearest U.S. government agency or representative.

From the U.K. viewpoint, this is working satisfactorily. And over the years of hand-carrying classified documents over national boarders as far as I know, there have been no known instances whereby the system or any classified documents have been conpromised The procedure required strict compliance with the rules and works well. This procedure is only extended for use when the transmission of classified material is time-sensitive.

Apart from this particular MLRS application, there's a genuine need to speed up the general transmission of bulk classified documents between firms by identifying and removing the sticking points in the systems on both sides of the Atlantic.

In these days of high technology and rapidly developing automated office systems, the security controller is frequently asked to advise on the availability of secure Telex and facsimile systems, which would speed up the transmission of classified information and documentation, particularly in the area of international collaborative projects.

The proposition has been raised with our authorities in MOD(PE) who in turn are talking to your authorities. But we understand at the moment that secure facsimile links would be technically impractical because of incompatibility of respective encryption systems and the need to transmit on a government-to-government basis. However, secure Telex facilities are considered a practical proposition. Security safeguards can be built that could satisfy the government-to-government requirement.

I have dealt with only a few of the defense security procedures associated with international collaborative projects. I hope it will stimulate discussion and emphasize the need for more flexibility in existing security procedures that could have an effect on other related security activities.

The restrictions placed on defense contractors by way of specific security procedures currently in operation do not appear to take cognizance of other disciplines imposed by governmental contractual conditions, i.e., the need-to-know principle, and the national disclosure policy — in your case DD Form 441 which states among other matters, that "whereas the parties desire to define and set forth the precautions and specific safeguards to be taken by the contractor and the government in order to preserve and maintain the security of the United States through the prevention of improper disclosure of classified information derived from matters effecting the national defense."

Mr. Bagley: Our next speaker from Marconi Electronics is James Wyatt.

Mr. James E. Wyatt: I'm going to talk about problems, so we can work on the problem in dealing

specifically with a U.K. company that's located in the United States and owned by a U.K. company. Such a company is Marconi Electronics. Mr. Robert White, who's from Cincinnati Electronics, will be helping me. I want to give an overview of the problem and have Bob come on with some real world experiences, and then I'll come back and try to draw some conclusions and give some possible recommendations.

As an overview to clear your mind about the organization — the General Electric Company of the United Kingdom is the owner of about 100 companies worldwide. One of those companies is the General Electric Company (GEC), Marconi Electronics Limited.

There is the Marconi Company. Canadian Marconi is owned 51 percent by GEC, and Marconi Avionics. The U.K. companies have Marconi Avionics in Atlanta, Marconi Electronics in Arlington, and in March of 1981 we bought Cincinnati Electronics.

For Mr. Earl Clark this will be a review. We visited the National Security Agency (NSA) on the 11th of March just before buying this company. NSA have been one of the easiest organizations to work with in obtaining information. Where the policies and procedures are perfectly clear, we are able to get clear-cut answers, so I want to thank NSA.

We're going to talk about the real world. Mr. White will give some specific examples of what's happening now. The problems that we're citing are not meant to be critical but only to tell you what's going on so that together we can solve them. We hope to learn what the environment is and to find a way to proceed.

Our goal is mutuality. We have been working with the Office of the Secretary of Defense, and we hope to do that in the future so that mutually whatever we provide can be accepted.

We went to visit a significant number of DoD activities before the Marconi Company acquired Cincinnati Electronics. After the aquisition, we received what we considered to be an immediate rejection. Rejection from what?

We received generally favorable comments about buying that company and operating under U.S./U.K. reciprocal clearance. We could not go into specifics, but everyone indicated that if we were to purchase the company and operate under the rules and regulations that it would be a viable operating organization. We were immediately very confident. After a few months our concerns were very guarded, and suddenly there was an area of grave concern. In my years as a program manager, I found this to exist in every program in which the government awarded to industry. Now we're trying to define the requirement and how we're going to make this thing work, and I think we're getting there. And this time when we get back up to the wild enthusiasm we hope we can stay there.

There were two alternatives open to us because these are companies that have been operating under the U.S./U.K. reciprocal clearance. The first alternative was to do *nothing*. Having been in the DoD, I recommended that we attack this thing head-on because our confidence in the DoD made me feel that we could arrive at a solution to this particular problem because we felt that it was inappropriate to try to operate on an individual-to-individual basis. We felt that many people will probably get into security situations that would jeopardize both governments as well as the company, so we did something.

We made a head-on, methodical attack. We documented a thick file, which Mr. White is going to talk about. We provided specific cases to the Office of the Secretary of Defense (OSD). Our attitude was one of "no surprises to the government." We talked with the people in the government who manage this particular situation. The approach has been very low key, and it has been a company to OSD problem. We felt it was appropriate to operate from the company to OSD before we tried to make it a government-to-government situation. The policies that have been agreed upon between the two governments are excellent; it's the implementation that's caused us the problem.

It's a complex subject. At the OSD level there is the security policy organization, of which Arthur F. Van Cook is a part. And his boss is on the same level as the man who is responsible for interna-

tional cooperative programs. So if there is a difference of opinion of the people, or a difference in objectives that they're trying to achieve, it becomes very difficult. In many organizations, horizontally and vertically, it comes all the way down the line to you, the security manager, in the company or in the government activity. The policy has been excellent but the implementation has not been good because it is a new thing that we're working toward.

Very few people know the total spectrum of this whole thing. I have worked the proplem extensively for the last year. I thought I knew all aspects of this until I had a meeting with Mr. Van Cook, who pointed out something to me that sent me into a state of shock. But thanks to Mr. Van Cook's patience, we're going to work out that problem. In general the results of any discussion ends up being a subjective assessment of what the situation is, but now we're getting down to an objective basis upon which we can talk.

The problem is difficult. I mentioned the various organizations that are involved. We have very few problems with the security people because you know what the regulations call for. The problem comes with the acquisition managers, with the contracting officer, and the people who are placing contracts because they do not know how to deal with companies that have the U.S./U.K. reciprocal clearance. There are different levels of understanding, different objectives, and the lines of communication are difficult.

You have heard about the voting trust which appears to be the simple solution to a foreign company. You may know that Magnavox Corporation belongs to Philips of Netherlands. Magnavox is just like any other U.S. company. The problem is Philips Corporation only reaps the benefits of the profits of Magnavox. Under the voting trust you have loss of control.

That loss of control is very important to us because when we bought Cincinnati Electronics the bank had just canceled the line of credit. The company was $8 million in arrears to suppliers. They had just missed two payrolls. Our company stepped in and made the payroll, and we had to put $16 million into that company to bring it up to par. I would suggest that it would not be a prudent management decision if you are buying an organization to say, "I don't want to have anything to do with the day-to-day control of this company." We found that it was necessary to organize under the U.S./U.K. reciprocal. That's why we have not gone to the voting trust. On September 17 after much discussion with the OSD we sent a letter to the OSD. It was very difficult finding out to whom we should address that letter. We finally addressed it to the acquisition side. We did that because we felt that side of the house knew less about the subject than the security side of the house. We wanted to force interaction between the two.

We've had four meetings with OSD. One of our company chairmen met with General Stilwell on November 12. We've had three more separate meetings with OSD. There has been progress and understanding. Both agree that it's not a simple solution, and we continue to work at the problem. While Mr. Van Cook's side of the house has provided their input to that letter, we hope that we will receive a position answer soon to our September 17 letter. We just want to make the current policy work; we don't want to change the policy. We understand the national disclosure aspects of what's going on.

Mr. White's presentation will show lack of consistency among the various activities with who, we have to work, and that's all we want to get at — consistence. Because it's not until we have consistency that we are able to determine whether or not Cincinnati Electronics can operate viably in this process under the U.S./U.K. reciprocal agreement. If we find that it can't, then we'll go to the voting trust. Mr. White will speak now, and I'll come back and try to draw some conclusions and give some recommendations.

Robert J. White: We were bought, and we became Cincinnati Electronics (CE) in March of 1973. The purchase by Marconi took place on March 31. At that time we had 43 active classified contracts in the house. At the time the clearance was invalidated by DIS on April 8, none of the contracts had been pulled back, none of the information had been requested to be returned except for one Request for Proposal (RFP) work statement that was in process.

I want to call to your attention what the ISM defines as a foreign national. It's any person not a citizen of, not a national of, nor an immigrant alien to the United States.

The general areas of our problems are in the areas of RFP's, procurements, information symposiums, data banks, and visits. I'll start with our first case.

1. CE had developed and delivered five engineering (EW) models of a system including the technical manuals, one of which was classified. That was in 1977. Participation was denied in the subsequent RFP for ten units although no significant new technology was involved. The production information was classified Not Releasable to Foreign Nationals (NOFORN). We believe it was because of the unacceptability of another company under foreign ownership. The application of this program was known from the original master security guide which was in-house.

2. We had a follow-on procurement to a program that we had participated in, having designed and developed a system several years ago, that had already been previously released to another friendly power. There was some action in the procurement area to reevaluate it for a NOFORN caveat. Just before my leaving, we successfully overcame that. But we had our fingers crossed going into DIS because it represented a significant amount of the income of Cincinnati Electronics Corporation.

3. In a similar case where we had gone many years in this particular type of procurement, we took the procurement activity through the right channels. Fortunately on this one, we were able to continue to work on the production follow-on, but it went through a long chain of events that took about three months.

4. We had a case of an RFP that was sent to Cincinnati Electronics Corporation, via the British Embassy, where it was misplaced for several days. A copy of this RFP also went overseas, both having followed the normal off-shore method. We finally got the RFP.

5. We had a contract involving a NOFORN caveat at the time of the sale, that was removed within two weeks after the sale of the company. However, to this date the authorities on this program require that all our visits on this contract go through the British Embassy for verification. The embassy has no knowledge of it nor is it in a position to verify or assure the security clearances of any U.S. citizens that are granted clearances by DISCO, which represents this case.

6. There was another contract that involved our people going to another user agency to perform the test on the equipment that we had developed. We also had all the data. We were required, according to the specification in the contract, to send a visit request through the British Embassy. The DD Form 254 specifically states; "there's no additional release of information involved, and no security requirements over and beyond paragraph 2-114 of the ISR." This again was an RFP. We were advised that there was going to be a critical nuclear weapons design information CNWDI and RESTRICTED DATA caveat on the follow up. We challenged the caveat. Both were removed or no longer required on the program. It was never in a DD 254, and never a part of the master security guide.

7. These concern several of the visits that we had. We run the gambit on visits from "no problem" to "no way". We've had elements within different elements of the same base making decisions on policy for the visits at that base. We were told that reciprocal clearances as far as visits are concerned are no different than any other visits. Disclosure or access are the concerns. We've had need-to-know certifications approved, but they were denied at the base being visited.

8. On one occasion an employee of ours gave

a presentation, and then he was told to leave because he had no business being there. The reasons were left unanswered other than the fact that he was determined to be a foreign national.

9. One contracting officer refused to certify the need-to-know for our project people to discuss the project at another facility that had already been visited. This was an after-the-fact request. He decided not to certify it, and the case is in limbo. The visit had already been made.

10. The Technical Abstract Bulletin (TAB bulletin) of the Defense Technical Information Center (DTIC) is in regard to information. The most serious concern of ours is the ability to obtain information and data in order to service DoD on future programs. Without it, we're dead. After some consideration, we were eventually approved to again receive the TAB bulletin. Access to the publications is another matter. Even on contracts where access is permitted by the DD 254, on many occasions the action of receiving the documents has been delayed beyond the usability data that we needed them.

11. Participation in the potential contractor program has been denied apparently because of foreign ownership, but no specific reason has been given although we've asked several times.

12. Attendance at symposiums has been denied almost entirely. Some of the reasons were: The information to be discussed may concern information not releasable; EW information is exempt from reciprocal cleared facilities; the ground rules for access state that all missile defense information is not releasable, and we do not have the staff personnel to screen the data to determine what is releasable or nonreleasable. You may be able to participate as a subcontractor On one program in another case, an employee wrote the technical paper, which was later determined to be NOFORN. He couldn't get to the base to deliver the paper.

These are a few of the cases that we have been trying to work out on an individual basis. It becomes quite an effort from our standpoint because we have other duties as far as security is concerned within the facility. Now Mr. Wyatt will tell what we are doing about it.

Mr. Wyatt: this problem clearly has to be broken into two portions. One is the visit clearance itself, and the other is information access. We've used the term "classified information" and "restricted information." In many cases we've had categorical denials on unclassified information because the government individual simply said, "There may be something in this unclassified information which you probably should not know." We're asking that it should be possible for some kind of determination to be made.

And finally, U.S. citizens with reciprocals are being treated as foreign nationals. Whether that should or should not be is not quite clear in our minds because there is some reference in the ISM about people representing companies of foreign interests, etc.

Some insist that visit clearances flow through the British Embassy. The only point that we're making here has been made by Mr. Van Cook. Our clearance is validated by DISCO, and the British Embassy has no knowledge of the security clearance of Cincinnati Electronics or the personnel associated with it. Some of the organizations operate in accordance with the ISM and others do not. In general visits between contractors have not been a problem because they are normally unclassified visits.

We're simply recommending that we be treated as *category one,* and we believe we have documentation in our hands where DIS suggests that we should be. Because we are a U.S.-U.K. reciprocal U.S. company incorporated in the U.S., we should be treated as *category one.* There may be some data on that, and I hope that matter can be cleared up as we begin to discuss this issue. If so we think that there simply needs to be emphasis on existing policy. If we are not treated as *category one,* we think that there's a case that can be built for the company being treated as such because of the way that the clearances are approved by DIS.

The categorical denials bother us. Were synonymous with NOFORN. We believe with the current system there has to be a case-to-case review. And that's where we have success with the NSA because each case which involves them normally is at Fort Monmouth. They expeditiously go to the NSA and expeditiously answer, so things flow very well. There is no single point of authorization, and that's something we have to work on. Contractors actions are normally based on unclassified or what the government says.

We're asking that the foreign disclosure decision be made up front. On every major system where there's a decision coordinated paper developed by the program manager and goes through the Army Security Agency Review Committee (ASARC) and Defense Security Agency Review Committee (DSARC) process, there are many decisions made about who can participate in the program. The small business decisions are made, and the minority company decisions are made. We're asking that the foreign disclosure decision be made and that it be disseminated with all of the other documentation so that the procurement activity then has a guide for making its decisions.

We also think that a denial has to be elevated to somewhere at least in the headquarters of the military department. As a program manager of the Army, I was going to make decisions which were completely on the safe side and had nothing to do with the total international cooperation. I was going to make it in the interests of what I was doing at Fort Monmouth. We think that the cooperative agreements have been made at a high level, and denials should be at the same level. The denials we have received have been made by the program managers.

Problems exist and we need better understanding and communications. We think a mutual solution can be reached. We don't want to change the security, we just want to make the policies work.

PART TWO

Annual Report

and

Selected Papers

1982

18TH ANNUAL MEETING

1. The meeting was called to order at 9:00 a.m. on May 25, 1982, by James Buckland, Seminar Chairman, who turned the meeting over to NCMS President James Mathena.

2. NCMS President Mathena opened the meeting. Dr. Edgar Hill, Director of Security for the Ministry of Defense, Procurement Section, United Kingdom, who is retiring from service this year, presented a gift of appreciation to President Mathena "for current and future proceedings of this Society."

3. Vice President and Membership Chairman Clarissa De Angelis presented the membership report. As of May 20, 1982, total membership was 567; 554 regular members; 8 at-large members, 1 honorary member, and 4 international members. There are 397 members from industry, 149 from government, and 21 others. There are 380 males, 187 females.

4. Treasurer Pamela Hart presented the Treasurer's Report. Receipts to date were $25,898.45. Expenditures to date were $6,228.95. There are still some outstanding bills for three bulletins and last year's journal. The Society had a net worth of $46,609.76 as of May 25, 1982.

5. The Finance Committee's auditor's report was presented by Gerald Berkin.

6. The Chairman of the Nominating Committee, Jack Robinson, presented the results of the election to the Board of Directors. Elections completed by May 10, 1982, for three-year terms as directors were: Clarissa De Angelis, James Maneggie, James Mathena, and Sandra Waller.

7. The newly constituted 19th Board of Directors held a meeting on May 24, 1982, to elect officers for the forthcoming year. Results are:

   President — Clarissa De Angelis
   Vice President — John Puckett
   Secretary — Sandra Waller
   Treasurer — Pamela Potter Hart

8. NCMS presidents for the past twelve years were in attendance and were introduced: Eugene Suto (1971, 1974); Jim Bagley (1972); Fred Daigle (1973, 1979); Jack Robinson (1975); Dean Richardson (1976); James Buckland (1977); Alan Thompson (1978); Marilyn Griffin (1980); and Chris De Angelis (1982).

9. Awards were presented to:

   Clarissa M. De Angelis "for her outstanding contribution to the Society as a member of the National Board of Directors during the period 1979-1982. During this period Ms. De Angelis served the Society with distinction in several positions including chairperson of the Membership Committee, member of the Executive Committee, National Treasurer and National Vice President."

   Robert Green "for his outstanding contribution to the Society as a member of the National Board of Directors during the period 1979-1982. During this period Mr. Green served the Society with distinction in various positions including chairperson of the National Education and Training Committee and member of the Board of Directors."

   James A. Maneggie "for his outstanding contribution to the Society as a member of the National Board of Directors for the period 1979-1982. During this time Mr. Maneggie served the Society faithfully as chairperson of the Awards Committee, member of the Industrial Security Committee, member of the Executive Committee, and National Secretary."

   James Buckland "for his outstanding contribution to the Society as a member of the National Board of Directors during the period

of 1980-1982. During this period Mr. Buckland served with distinction as chairperson of the 1982 National Seminar, as a member of the Industrial Awareness Committee, and as a member of the Executive Committee.

10. International members in attendance were introduced: Robert Grogan, Canada; John McMichael, U.K.; William Tremble, U.K.; and Edgar Hill, U.K.

11. Arthur Van Cook, who is retiring, received a plaque from the NCMS for "your decades of dedication to the Information Security Program and its effective implementation, your service in the Society as a chapter chairman and to it as an authoritative and informative speaker at countless national seminars, your continuing encouragement to the Society and its participation toward effective implementation of several information security programs, as well as your willingness to listen and use its constructive recommendations when possible. For these reasons among many, NCMS extends its appreciation, thanks and very best wishes."

12. Closing comments by Mr. Mathena; The Society had a very active year. We continue to increase our membership thanks to our Executive Secretary Eugene Suto and his assistant Barbara Suto, who did a tremendous amount of work in this area.

    The Board of Directors of the Society was very active in reviewing policy and regulation changes with the new Executive order and DoD 5200.1R. It was a rewarding year for the Society. As President, I received tremendous support during the past year, and I wish to thank the Board of Directors, Executive Secretary Eugene Suto, our Publications Director Jack Robinson, Directory Editor Virginia Kempton, the chapter chairmen and area coordinators who worked hard to advance the goals of our Society, our members who worked hard in recruiting new members, and James Buckland, chairman of this seminar.

    The opportunity and pleasure of being an NCMS President has been gratifying, especially the close association with so many dedicated individuals.

    In closing, I would like to encourage the future participation of our many new members. You have the opportunity to participate or serve as a chapter officer or a chapter chairman. It can be beneficial for your personal development, your company, your agency and your Society.

    I also would like to encourage you to continue your efforts in recruiting new members. The stronger we are, the better our programs will be; and we will all benefit.

13. Since there was no further business the meeting was adjourned.

*INTERNATIONAL COOPERATION**

James J. Bagley
R.B. Associates, Inc.

It is a distinct pleasure to be with the Guild of Security Controllers at the kind invitation of your chairman. I would hope that a result of this meeting would be further cooperation between NCMS and the Guild which, in turn could be a vehicle for closer cooperation between our governments.

I have been involved in international cooperation in one way or another for nearly 40 years and in a variety of capacities. Today I am representing the National Classification Management Society (NCMS) on the one hand, and on the other presenting my views of the background, present problems and the possible future of U.K. companies or U.K. owned companies doing business in the U.S. There access to defense information, the DoD and the military departments and defense industry is a requirement.

The following topics will provide the framework for discussion:

- NCMS - Its Role and Influence
- International Cooperation
  - The U.S. National Disclosure Policy
  - Technology Transfer
  - Export Controls, the ITAR, COCOM
- Foreign Ownership, Control and Influence DoD Reciprocal Clearances
- Acquisitions - The "Booby Traps"
- The Future (Prayerfully)

NCMS was started by interested people who were involved in the then arcane world of security classification - personnel of the Atomic Energy Commission. Early in 1963, these people recognized there was a need for improving communications between the classification people of the nuclear design laboratories and those in the production facilities. A meeting was held and the idea evolved that what was needed was a professional group made up of practitioners in both government and industry. Because the people were technically oriented and familiar with technical societies it was natural that they thought in terms of a professional society which could serve as the sounding board for advancement of this arcane art as well as the training ground for professionals.

In the early discussions the idea of associating with the existing American Society for Industrial Security was set forth. That approach was not productive. DoD officials were highly receptive to the idea of a professional society and became involved in the necessary organizational steps.

The Society was incorporated as a non-profit professional society and a Charter was issued by the State of New Mexico. Under the leadership of interested persons - government and non-government chapters were formed in Washington, D.C., the San Francisco Bay Area, Southern California, the Rocky Mountain area, New England, and a Mid-Eastern chapter spearheaded by Jim Moran now with DIS, Brussels.

The first Seminar was held in the State Department in 1965. The quality of the program and the eminence of the speakers set the stage for the standards which have continued to this day. Some of the speakers were:

> The Chairman, Subcommittee on Foreign Operations and Government Information, House of Representatives**
>
> The Assistant to the Secretary of Defense for Atomic Energy
>
> The Deputy Director of the U.S. Arms Control and Disarmament Agency
>
> The Deputy Assistant Secretary of Defense (Security Policy)

Since its establishment, NCMS has been in the forefront of questions relating to classification, security, intelligence and a variety of other subjects. It has:

---

*Presented at the Annual Meeting of the Guild of Security Controllers, United Kingdom, October, 1982.

**John E. Moss, father of the U.S. Freedom of Information Act

- Participated in the drafting or the amendment of Executive Orders on National Security Information and Intelligence on invitation by the DoD or the National Security Councils (or not, as a given case may be) in the administrations from President Johnson to President Reagan.
- Participated in the drafting of the regulations of the Information Security Oversight Office (ISOO) (and its immediate predecessor, the Information Classification Review Committee).
- Provided requested recommendations on the Charter of operation and the organizational placement of the ISOO.
- Participated in the drafting of the DoD and departmental directives/regulations on information security as requested.
- Provided requested comments on the investigations and surveys of the U.S. General Accounting Office (the investigative arm of the Congress) on the government information security program and guidance given to contractors.

It is surveying the effectiveness of Special Access Programs where the security aspects are outside the purview of the Industrial Security Program. Some members of NCMS are involved in that examination.

- Developed criteria and standards on how to write security guidance.
- Participated in and critiqued the pilot model of the training program developed by the Defense Industrial Security Institute.

Some of the important and relevant subjects covered by NCMS seminars and mini-seminars are displayed in Table 1.

TABLE 1
SEMINAR TOPICS

SECURITY CLASIFICATION IN RUSSIA, 1968

THE EFFECT OF CLASSIFICATION ON THE DISSEMINATION OF TECHNICAL INFORMATION, 1968

COMPUTER SECURITY, 1966 (AND SUBSEQUENTLY)

THE BRITISH OFFICIAL SECRETS ACT, 1972

AUTOMATED DOCUMENT CLASSIFICATION SYSTEM, 1970

FREEDOM OF INFORMATION VERSUS CLASSIFIED INFORMATION, 1968

INTERNATIONAL SECURITY, 1974

THE LEGAL PROTECTION OF COMPUTER PROGRAMS, 1965

NUCLEAR SYSTEMS FOR THE FUTURE OF SPACE FLIGHT, 1966

THE PENTAGON PAPERS — WHO WON, 1974

SECRECY, PRIVACY AND THE COMPUTER, 1975

U.S. CONTROL OF NON-CLASSIFIED INFORMATION AND COMMODITIES, 1971

SECURITY CLASSIFICATION MANAGEMENT AS PRACTICED BY OTHER GOVERNMENTS, 1971

THE PROTECTION OF COMPANY PROPRIETARY INFORMATION, 1965

FREEDOM OF INFORMATION AND THE BRITISH OFFICIAL SECRETS ACT, 1979

THE CANADIAN SECURITY CLASSIFICATION SYSTEM, 1979

Because of its relevance I have brought with me the Table of Contents, the Foreword and Concept of the 13th Seminar. The principal speakers were the Chief Scientists of the Defense Intelligence Agency, the Army, Navy and Air Force, and the Defense Advanced Research Projects Agency. As well, the Archivist of the United States — the nation's record keeper, were the Chief Counsels of Committees of the House of Representatives and the Senate.

The concept of a major training exercise conducted during that seminar was to classify and provide guidance for a weapons system from the prime contractor down to the second tier subcontractor. The system proposed was a tank system with a gun system capable of first round on target all-weather; a laser target designator; a communication system crypto-secure from the internal communications within the tank, from the tank to the local support troops; secure communications to battalion, regiment, division, corps and army levels; also a secure satellite communications capability. A complicated exercise, obviously, but the system was entirely within the state-of-the-art.

In sum, NCMS is a singular force in the classification process. It has produced the most significant and generally the only literature available on the classification process. The members include individuals from the three branches of our government, the intelligence and security agencies and industry. Industry, in accord with U.S. definition, includes the academic community involved in defense research. NCMS members are involved in the development of policies and procedures for government and industry usage, on orders and directives, legislation, procurement, research, intelligence, security, recordkeeping and the production of records. NCMS is recognized as the voice of reason in problems which, though often timeless, become part of public debate.

The society provides a forum for the advancement of preliminary proposals which could not otherwise be studied or debated dispassionately. Through the chapter process concepts can be proposed, studies, voted up or down, or modified. It has been the vehicle, through its publications, seminars, mini-seminars and meetings by which the membership becomes aware of situations which later become problems.

The later point, parenthetically, probably is the reason why I am here; to make you aware of some very pressing problems which must be equitably resolved. And, computer security was discussed long before it became an official problem; the effects of the Freedom of Information Act on classification was discussed within two years of its passage. So that is a short version of NCMS. Being a Life Member of the society, I am proud and honored to be a member.

I would hope that one of the results of this meeting would be a greater participation by both of our societies on subjects which affect both of us. In recognition of the increase in international cooperation, the NCMS bylaws were amended to offer membership to individuals who meet the membership qualifications and "are employed in or by a country or facility with which the U.S. has a recognized security agreement and/or has a facility clearance granted and/or recognized by the U.S.". there are now Guild members who are also members of NCMS and we of NCMS hope that the Guild could open its membership to NCMS members.

In the final analysis, it is we who are faced with the difficulties of interpreting wisely, and enforcing judiciously, those laws and regulations affecting security problems. Recognizing this, NCMS stresses the training and education of its members who are faced with problems requiring timely solutions. Together we can take a giant step by taking a joint look at mutual situations.

International Cooperation

Turning now to the general — and particularly vexing — subject of International Cooperation.

The U.S. foundation of international cooperation (since World War II) is the National Disclosure process which evolved from the enactment of the National Security Act of 1947 (PL 253, 80th cong, July 26, 1947). that statute established the National Security Council (NSC), the Director of Central Intelligence and Central Intelligence Agen-

cy and the Department of Defense. The NSC is charged "to assess and appraise the objectives, commitments, and the risks of the United States in relation to our actual and potential military power, in the interest of national security, for the purpose of making recommendations to the President in connection therewith; and, to consider policies on matters of common interest to the departments and agencies of the Government concerned with the national security, and to make recommendations to the President in connection therewith."

Figure 1 and Table 2 display the organizations for general membership of the related councils. There are "special" members invited as appropriate. One common one, unsurprisingly, is the Director of Central Intelligence.

TABLE 2

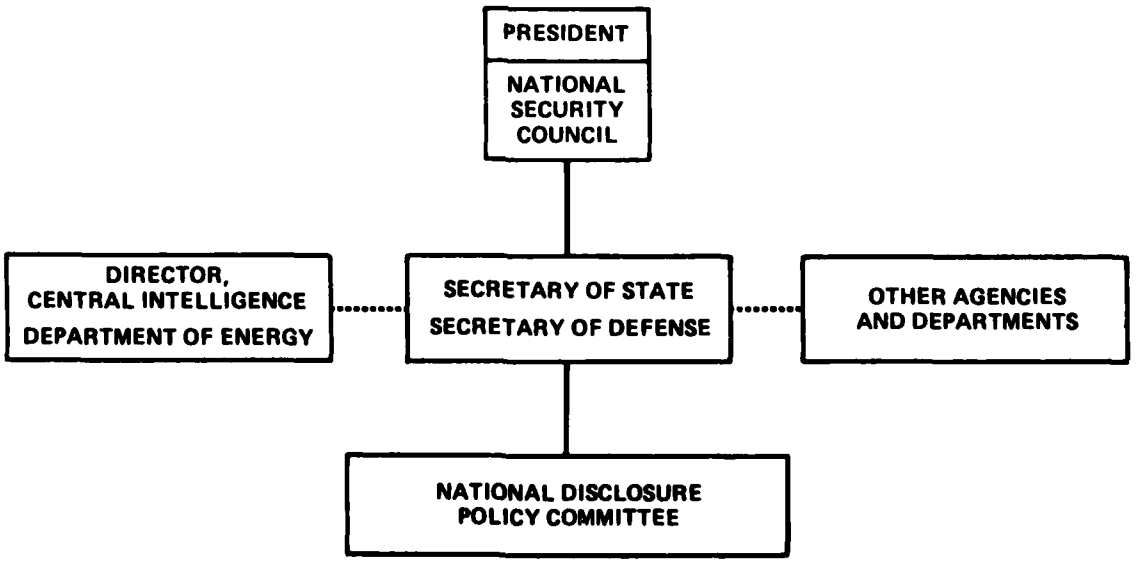
NATIONAL DISCLOSURE POLICY
NDPC
GENERAL MEMBERS

DEPARTMENTS OF

- STATE
- DEFENSE
- ARMY
- NAVY
- AIR FORCE

JOINT CHIEFS OF STAFF

NATIONAL DISCLOSURE POLICY AUTHORITY



..... COORDINATION

FIGURE 1

Then Table 3 discribes the criteria to be met in a case of foreign disclosure. You will note a few points. The authority rests with the President effected through the National Disclosure Policy Committee, chaired by DoD. A critical criterion is that the recipient will afford the information substantially the same security protection: I will not attempt to define "substantially"; it is sufficient to say that Agreements between countries set the limits and mutually acceptable requirements for compliance.

I would note, parenthetically the differences in meanings of common words between English/english and U.S./english. Would that there were a common dictionary. However, such an undertaking would take years to work out and eons before general acceptance. I am reminded of the current

TABLE 3

NATIONAL DISCLOSURE POLICY
CRITERIA

- DISCLOSURE IS CONSISTENT WITH FOREIGN POLICY
- MILITARY SECURITY OF U.S. PERMITS DISCLOSURE
- REC'PIENT WILL AFFORD INFORMATION SUBSTANTIALLY THE SAME SECURITY PROTECTION
- LIMITED TO INFORMATION NECESSARY TO THE PURPOSE OF DISCLOSURE
- DISCLOSURE WILL RESULT IN BENEFITS TO U.S. AT LEAST EQUIVALENT TO VALUE OF INFORMATION DISCLOSED

arguments in the United States on the "updating" of the King James version of the bible — a bruising battle.

Table 4 lists the categories of information which *generally* are exempt from the Policy. You will note however, that some of the exemptions are covered in separte agreements authorized under our laws. Forexample, the 1954 Amendment to the Atomic Energy Act of 1946 (PL 703, 83d Congress) permits the exchange of atomic information with certain countries, with strict limitations. Section 123 of the Amendment requires that no cooperation with any nation shall be undertaken until the President approves the safeguards and guarantees required by the law and i.. ..reed to by the cooperating party.

TABLE 4

NATIONAL DISCLOSURE POLICY
CATEGORIES OF INFORMATION EXEMPT FROM NDP–1

- NATIONAL INTELLIGENCE
- COUNTERINTELLIGENCE PROGRAMS & PRODUCTS
- COMMUNICATIONS SECURITY INFORMATION & MATERIEL
- COMMUNICATIONS INTELLIGENCE/COMMUNICATIONS INTELLIGENCE SYSTEMS
- ATOMIC INFORMATION
- STRATEGIC PLANNING & GUIDANCE

As you know, there are agreements in place between the U.S. and the U.K. on some of the exempt categories of information. Also, there are certain categories of information authorized for release to one country and not another. For example, the treaty between the U.S. and Canada permits the exchange of some information which would not be releasable to the U.K. Similarly, I am sure there are agreements between the U.K. and Canada on some information which would not be releasable to the U.S.

How does the disclosure process work? In practice, authority to release DoD information is delegated to the Military Departments and major DoD agencies for information under their purview. These departments and agencies, in turn, may redelegate release down one level; say to a Systems Command, or the Program Manager of a major program much as Trident, for example. Further re-delegation is not authorized. The departments then establish the kind and levels of information which may be released. The types and levels of information which may be released is set down in an Annex.

Figure 2 is adopted from the primary annex also called "The Chart" in National Disclosure Policy terms. However, within these categories may be detailed descriptions along with agreements on specific subjects: laser research, surface or air radar, specific types of equipment to meet operational requirmeents, etc.

ANNEX TO NATIONAL DISCLOSURE POLICY

CHARTS

		COUNTRY A	COUNTRY B	COUNTRY C
ORGANIZATION, TRAINING AND EMPLOYMENT OF MILITARY FORCES	1	S	C	
MILITARY MATERIEL AND MUNITIONS	2	S	C	
APPLIED RESEARCH AND DEVELOPMENT INFORMATION AND MATERIEL	3	C		
PRODUCTION INFORMATION	4	C		
COMBINED MILITARY OPERATIONS, PLANNING AND READINESS	5			
U.S. ORDER OF BATTLE	6			
NORTH AMERICAN DEFENSE	7			
MILITARY INTELLIGENCE	8	TS	S	X

FIGURE 2

Each Department, in turn, publishes directives that further refine the categories and detail the departmental policies on such subjects as: the information which may be released by operational commanders, the release authority of Systems Commanders and other commands which have been delegated disclosure authority. Also covered are policies on the exchange of personnel, visits, releases to international organizations and staffs, releases to liaison officers assigned to commands. Generally within determined Disclosure Policy a Systems Commander has authority to release information under his exclusive cognizance — he "owns" the information, has produced it or has authorized its production. This is in contrast to the authority to release information under his control. He may well have custody over much information under the cognizance of others which he has no authority to release without the specific approval of the originator of that information.

Illustratively, information of interest to or originated by another department or agency must be approved for release by that department or agency. As you can imagine, there is little information under the exclusive control of one department and therein lies no small problem of timing and coordination. It would be common, for example, that a report on surface to air radars would be of interest to all the military departments. A compendium of reports published by one command or activity containing abstracts or briefs on a variety of subject areas would require the release approval of *each* originator.

The National Disclosure process is fundamental to the problem of doing business in the U.S. Information requested may not be released until a decision is made that it has been released, or is releaseable to the requesting country. And it is quite likely that the persons considering the request may not know whether the information has been released or is releaseable. That the system is complicated is an understatement.

Figure 3 shows DoD's policy players. Observable is the two-sided process. The responsibility is divided between the Under Secretary of Defense (Research and Engineering) and the Under Secretary of Defense (Policy). Within each of these houses, responsibility is further divided. This may best be described when you realize that a typical program is governed by the following processes: Research and development, acquisition, security, intelligence, procurement, departmental and national policies. Each is governed by a set of regulations issued by ascending levels of command and, at each level, the popular politics of the day. It may be of interest to note that I have identified 35 DoD directives relating to international cooperation. To this must be added the Departmental directives of the Army, Navy and the Air Force which implement, and sometimes refine application of these directives. Carrying out the national disclosure policies is indeed a Pandora's box.

Technology Transfer

Technology transfer has been the favorite "whipping boy" of both the liberals and the conservatives (our variety) for many years. The cries: The U.S. is giving away too much; the fruits of U.S. research and development should be made available to all: the dissemination of technology developed privately should not be controlled; the products of U.S. industry should be made available to anyone who has the price; the free enterprise system (whatever that is) should be free; to quote the King in *Anna and The King of Siam,* "et cetera, et cetera, ad so forth." There is an argument for every shade of political happening to be in favor at the moment.

Regardless of the position taken, seldom is there a consistency; each proponent uses seldom defined words; or defined so narrowly or broadly that the definition, if there is one, can apply to whatever position is being advanced.

You will be happy to learn that I am not going to become part of the semantics battle. I will not take a position one side or the other, but will address only that policy that has been consistent since the administration of President Truman and has not changed regardless of the party in office.

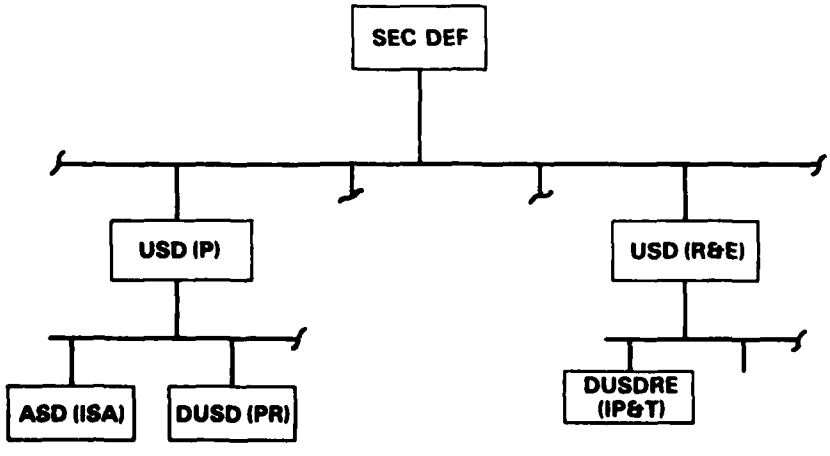


FIGURE 3

The United States policy objective is twofold — to facilitate international trade and to protect the national security through the control of exports.

Viewed, critically, a contradiction in the objectives is evident to facilitate and to protect. Let us examine the transfer problem. The current problems of technology have been with us since the days of the Cold War. As a result of the efforts by the Soviet Union to acquire access to important information by fair means or foul, enacted were the Export Control Acts of 1949 which remained substantially in effect until the enactment of the Export Administration Act of 1969 and its subsequent revisions. As we know only too well, advanced technology has become a target for acquisition; therefore, there is a need to protect some information from improper acquisition.

However, since time recorded at least, the world has changed dramatically. At this time the U.S. is no longer the world leader in technology. We have seen new plants, production facilities and facilities rise from the ashes of saturation bombing both in Europe and the Far East. From Hong Kong to Manchuria, to Korea and Japan we have seen the rise of new industries, technologies and ability. Even those countries now do business in the West for lower labor rates. At the same time we have seen some of our industrial leaders become more interested in a "fast buck" than in long term investment. We have also seen our traditional economies make a painful transition from producers to users — from the makers of goods to the providers of services. So, the U.S. needs the technical skills of others. Whether the need for those skills should become subordinated to current politics or philosophical discussions is not germane here. However, two facts are important.

First. The last two Under Secretaries of Defense (Research and Engineering) have reported to the Congress in their annual messages the relative standings of the U.S. to the U.S.S.R. in 20 of the most important technology areas. Displayed as Figure 4 is that list from the Fiscal year 1982 Report. Not shown of course — and something to ponder over — is the standing of the U.K. to the U.S.S.R. in those areas; nor is there a net technical assessment of the standings of the combined highly developed Western countries in these areas.

When looking at the list and considering the implications that can be drawn, I am also aware of a letter sent recently to the President of the National Security Industrial Association by the Deputy Secretary of Defense, Mr. Carlucci. Particularly noteworthy were two sentences which appear to strike at the heart of the situation it is describing — the decline of Quality and Productivity in the United States: "We believe that quality starts with an attitude, an essential attitude in the general atmosphere created by management. To be effective, quality must have continuous emphasis by corporate management.

Second. There is a substantial increase in international cooperation; there are approximately 43 General Security of Information Agreements in place or under negotiation or revision. There are some 20 Industrial Security Annexes to those Agreements in place or under negotiation.

Finally, notwithstanding the trials and tribulations of outrageous fortune — technology will be transferred, and regardless of the winds of change or the publicity of the day — whether the U.S. will or will not authorize it, or whether or not your companies will or will not be criticized for fulfilling their current contractual obligations, the exchange of information will continue as a matter of national policy, in my opinion.

The objectives of cooperation may be set forth as follows:

OBJECTIVES FOR COOPERATION

- Improve Western Combat Effectiveness
  - — Technology Sharing - Best Technology
  - — Interoperability
- Improve Resource Efficiency
- Strengthen Political/Economic Cohesiveness of the Free World

And, in the spirit of cooperation efforts to strike a blow at the "Not Invented Here" syndrome — endemic in both our societies — is described officially in DoD, thusly:

RELATIVE US/USSR STANDING – 20
MOST IMPORTANT TECHNOLOGY AREAS

	US+	US/USSR=	USSR+
Aerodynamics/Fluid Dynamics		X	
Automated Control	X		
Chemical Explosives			X▶
Computer	◀X		
Directed Energy			X
Electro-Optical Sensors	X▶		
Guidance & Navigation	X▶		
Microelectronic Mat'ls & Integrated Circuit Manufacture	X▶		
Nuclear Warhead		X	
Optics	X▶		
Power Sources (Weapon)			X▶
Production/Manufacturing	X		
Propulsion (Aerospace)	X▶		
Radar Sensor		X	
Signal Processing	X		
Software	X		
Structural Materials		X	
Non-Acoustic Sub Detection		?	
Telecommunications	X		
Hydro-acoustics	X▶		

Statement of the USD/R&E FY-82

FIGURE 4

FAMILY OF WEAPONS

- Split R&D responsibilities among countries for systems within a "family" of requirements
- Improves efficiency in Alliance
- Satisfies common national requirements
- Satisfies national industries' desires for share of market

Pride is still one of the capital sins, as you will remember. Production describes a present and growing approach to cooperation. One way to describe it is that one country develops or produces an item and offers it to another for production through licensing. Such an approach serves to *eliminate duplication* in Research and Development while fielding the latest technology systems in NATO — a problem that has become increasingly worrisome.

A special aspect of this approach is that of consortia. A number now exist and others are evolving. They achieve efficiency — especially notable is the independent European program Group. However, under this concept corporations from different countries are turning in proposals for new systems for multi-country application and production — as many, if not all of you know. I cannot resist saying at this point that we have been talking about interoperability and standardization for the last 35 years. Perhaps some of us, at least, will live long enough to see it.

Export Controls

There are two basic mechanisms by which the U.S. controls exports; Export Control Laws and the *International Traffic in Arms Regulations (ITAR).* Ancillary is the COCOM. To give you the flavor of the concern I will quote some words of Congress in the Declaration of Policy in the Export Control Act of 1969 (PL 91-184):

> "(1) It is the policy of the United States both (A) to encourage trade with all countries with which we have diplomatic or trading relations, except those countries with which such trade has been determined by the President to be against the national interest and (B) to restrict the export of goods and technology which would make a significant contribution to the *military potential of* any other nation or nations which would prove detrimental to the national security of the United States."
>
> "(2) It is the policy of the U.S. to use export controls (A) . . . (B) to the extent necessary to further significantly the foreign policy of the U.S. and to fulfill its international responsibilities, and (C) to the extent necessary to exercise the necessary vigilance over export from *the standpoint of their significance* to the national security . . ."
>
> (3) It is the policy . . . (A) to formulate, reformulate, and apply any necessary controls to the *maximum extent possible* in cooperation with all nations with which the U.S. has defense treaty commitments and (B) formulate a unified trade control policy to be observed by all such nations."

The control mechanism is COCOM (Coordination Committee), the process by which the NATO nations and others, meet periodically to decide which items are important to their collective defenses and which should be controlled through individual export limitations. Items are proposed and the committee meets to arrive at a decision. The process, which might better be covered by the rules promulgated by the Marquis of Queensbury, arrives at some sort of a decision and a list or revisions to the list are published which are subject to export restrictions. Whether the participants comply with the decisions, bend the decisions or ignore the decisions, are matters beyond the sensitivities of this sensitive body, and shall not be discussed. I am sure that each of us has our own opinions.

The Export Control Program is directed by our Department of Commerce through the Office of Export Control. That office makes a significant use of technical committees in its deliberations. For new articles, materials, or supplies, including

technical data and other information which are subject to export controls, or are being considered for such controls, the Secretary, at the request of industry or other interested parties, appoints a committee to ascertain world-wide availability, utilization of production and technology and licensing procedures, etc., to provide the basis for making a decision as to whether or not to limit exports.

There are specific procedures which govern the Export of Technical Data which are included in the publications of the Bureau of East-West Trade of the Department of Commerce and which are available. In general however, the rules are if the information is publicly available, an export license is not required. Otherwise a license *may* be required if the data pertains to an article which is controlled.

Data may be released in a number of ways under the laws. Lest there be any misunderstanding, legally information subject to the act and taught to a student in a school is covered.

TECHNICAL DATA MAY
BE RELEASED THROUGH

- Visual inspections by foreign nationals of U.S. origin equipment and facilities
- oral exchanges of information in the U.S. or abroad
- The application of personal knowledge or technical experience acquired in the U.S. to situations abroad

Be aware that confusion over what constitutes the re-export of data exists. This is the definition:

RE—EXPORT OF TECHNICAL DATA

"Re-export of Technical Data" means an actual shipment or transmission from one foreign country to another, or any release of technical data of U.S.-origin in a foreign country with the knowledge or intent that the data will be shipped or transmitted to another foreign country.

International Traffic in Arms Regulation

The Mutual Security Act of 1954 authorizes the president to designate and control the export and import of arms, ammunition and implements of war, including the technical data relating thereto. The responsibility for carrying out the requirements of the law is delegated to the Secretary of State, who, acts with the concurrence of the Secretary of Defense, and in some instances, the Secretary of the Treasury (principally on import cases). In practice, when a company desires to export, and is licensed to export, an Export License application is made to the Office of Munitions Control, State Department. The license then is forwarded to the DoD and the Military Departments for concurrence in the export, or for reasons why the export should not be made. You should be aware that the DoD and the Military Departments have a substantial role in the process. A negative vote can mean no export. If all goes well the license is issued and the export process proceeds.

There is a point, however, that should be understood; it is the cause of considerable misunderstanding. If the export (article or technical data), whether classified or unclassified, is the result of, in connection with, or related to a contract, Agreement, or Memorandum of Understanding, a license is not required. The Foreign Disclosure decision has been made. This shows the importance of the foreign disclosure decision and the absolute requirement that that decision be made as early as possible in the approval of any program.

What I have tried to present is a flavor of the complexity and interrelation of the various programs. And, why a security person who operates in the international arena must be conversant with the laws, regulations and procedures of foreign policy, international trade, procurement, security — obviously, technical data and all other information related to interactions among them. With all of this, there must be an understanding of the import of the technical elements of the exchange. All too often, whether an exchange will be approved or denied rests on a single technical point.

Foreign Ownership Control or Influence

Now, to the heart of this paper — FOCI. to begin, it is useful to discuss how foreign investment is

actually controlled in the U.S. The best source of this information that I am aware of is a report by the Department of Commerce of April 1976, entitled: "Foreign Direct Investment in the United States.", volume 7: Appendix K. Because of its important contribution to this field, some direct quotes are appropriate.

> "Whether any statutory controls directly restrict alien investment in the defense industry is uncertain. Rather, the main obstacle to alien investment in the defense industry is the industrial security program administered by the Department of Defense, which, although it does not directly restrict such investment, indirectly has and probably will have that effect in most instances."

This is control by indirection, admittedly. However, free societies often must use indirect means to achieve and maintain a viable and independent defense apparatus which is free from undue foreign influence.

At this point it is also useful to provide the official DoD definitions of Foreign Interest and Representative of Foreign interest. As found in paragraph 3ao and 3bw of the Industrial Security Manual for Safequarding Classified Information (ISM) they are:

> "**Foreign Interest.** any foreign government or agency of a foreign government; any form of business enterprise organized under the laws of any country other than the U.S., or its possessions; any form of business enterprise organized or incorporated under the laws of the U.S., or a state or other jurisdiction of the U.S. which is owned or controlled by a foreign government, firm, corporation or person. Included in this definition is any natural person who is not a citizen or national of the U.S., (an "immigrant alien" as defined in paragraph 3av is excluded from the definition of foreign interest.)"
>
> **Representative of a Foreign Interest.** Citizens or nationals of the U.S. or immigrant aliens who, in their individual capacity, or on behalf of a corporation (whether as a corporate officer or official or as a corporate employee who is personally involved with the foreign entity), are acting as representatives, officials, agents, or employees of a foreign government, firm, corporation, or person. However, a U.S. citizen or national who has been appointed by his U.S. employer to be its representative in the management of a foreign subsidiary (i.e., a foreign firm in which the U.S. firm has ownership of at least 51% of the voting stock) will not be considered as a representative of a foreign interest, solely because of this employment, provided the appointing employer is his principal employer and is a firm that possesses or is in process for a facility security clearance."

It should be emphasized that an employee of a U.K. company, who is a U.S. citizen is, in the eyes of the DoD and the Military Departments, a Representative of a Foreign Interest. Thus in all relationships with the DoD the person is considered a representative of foreign interest and handled as a foreign national even though the individual may hold a U.S. granted clearance.

Two basic options are available to a U.K. firm considering the acquisition of a U.S. company doing defense business; the Voting Trust and a Reciprocal Clearance.

To reduce several pages of legal jargon to understandable words, a Voting Trust is a process by which the owners place full responsibility and authority for running a company into the hands of at least three U.S. citizens, cleared or clearable, who operate the company. The Trustees are responsible to report to the owners only that information which is not sensitive, or not subject to any dissemination restrictions, or has been determfined to be releasable to the U.K.

The owners do not control, operate, or influence the company. They have given up their rights. There are examples of companies which operate under such arrangements — notably, North Amer-

ican Phillips which owns the Magnavox Corporation, a large defense contractor, is, in turn, owned by the Dutch Phillips company. There is a Voting Trust Agreement between the Dutch Phillips and North American Phillips.

The other option is a Reciprocal Clearance granted under the Industrial Security program, the terms of which are outlined in paragraph 31 of the ISM.

Table 5 shows the requirements of a U.K. firm which does defense business in the U.S. In all instances the firm would operate exactly the same as if it were located in the U.K. Clearances, accesses, visits, etc., would be processed through the Embassy. The procurement information it sought would, if otherwise restricted, would be obtained in the same way.

TABLE 5

U. K. COMPANIES DOING DEFENSE BUSINESS IN THE U. S.

- MOD MUST PROVIDE SECURITY ASSURANCE TO U.S.
- OPERATES LIKE A FIRM LOCATED IN THE U. K.
- MUST ORGANIZE UNDER U. S. LAW
- MAY BE SPONSORED FOR A RECIPROCAL CLEARANCE

Without dwelling on the legal aspects of doing business, an English firm operating in the U.S. would be incorporated in the U.S. and would pay the usual taxes — state, local and federal. If appropriate, and it was willing, the firm could be sponsored for a Reciprocal clearance. This means that someone in the DoD or a DoD activity would request that the firm be processed for a clearance under the provisions of the ISM. The justification would be the possibility that the firm would be awarded a contract requiring access to classified information as high as Secret. It would be unlikely that a clearance for access to Top Secret would be authorized.

DoD Reciprocal Clearances

Table 6 sets forth the DoD reciprocal clearance process. A request would be made by a DoD activity, or by a contractor having a contract which desires that a U.K. firm be a bidder. The request would be sent to the local regional DIS office for processing.

TABLE 6

THE RECIPROCAL CLEARANCE PROCESS

- CLEARANCE REQUESTED BY PROCUREMENT ACTIVITY
- VISIT BY DIS (IS) REPRESENTATIVE
- WHO IS CLEARED
- TIME REQUIREMENTS
- CLEARANCE ISSUED

A visit to the firm would be made by a local DIS person who would provide a long checklist of requirements. There is no difference between the requirements for a U.K. firm and a U.S. firm.

With U.K. firms there is always one sticky point. All the Directors and Officers must be cleared, except for those Directors (not Officers) who could be excluded from access to classified information by formal Board Resolution. All others who would require access in the performance of their duties would also be cleared. The long form DD 49 would be required. Depending on the cooperation of the people involved (and Corporate Board members are notorious for foot-dragging) the time required to process the clearance can be as short as a few weeks or may take longer than a year.

So a clearance is granted. What then happens to a U.S. firm, acquired by U.K. interests, which converts from a general to a Reciprocal clearance? Table 7 presents the actions taken by the DIS and the contracting activities.

TABLE 7

WHAT HAPPENS

- COMPANY NOTIFIES DIS OF THE POSSIBILITY OF ACQUISITION (during the negotiating process)
- ON ACQUISITION

  DIS suspends current clearance

  DIS notifies all procurement activities of acquisition (all open and closed contracts)

  Contracting Activity Action

  Continue or stop work on current contracts
  Retain or return or destroy classified holdings (confiscation a possibility)
  Cancel or allow current visit clearances
  Decide on future business

The first action is the suspension of the clearance in place. This is important because without a clearance, the U.S. firm cannot take on, or be eligible for new business.

The DIS will notify each contracting activity that the acquisition has been made and request disposition of each contract in place, or each concluded contract in which the retention of classified information was authorized. A listing of all current DD 254s (Contract Security Classification Specification) would be furnished. The contracting activities would then take the actions indicated. I emphasize that the contracting activity legally can take any of the actions indicated, because the basic contract agreement between the company and the government on the handling and protection of classified information would have been cancelled by the acquisition.

The new problems are obvious: A contracting activity may authorize the completion of a current contract or may cancel the contract and have all residual assets of the contract returned to the contracting activity. It may authorize the completion of an existing contract but bar the firm from competing on a follow-on contract for the identical item. Such a circumstance would be particularly damaging in the case of an advanced development contract to produce one or two items to prove feasibility, and if proven, would result in a sizeable production contract. This has happened.

These problems, in turn, lead to what happens to the company now in a new world, the least of which are the restrictions listed in paragraph 31 of the ISM. Table 8, "After Clearance Blues", sets forth the possibilities.

TABLE 8

AFTER CLEARANCE BLUES

COMPANIES WITH RECIPROCAL CLEARANCES ARE:

- CUT OFF FROM ACCESS TO:

  Procurement information - RFPs, IFBs, etc. (there are exceptions)
  Information Analysis Centers
  DoD Information for Industry Programs
  Symposia, meetings

- VISITS

  ISM (paragraph 37) Category 1
  Government activities - Category 4 (foreign nationals representatives, foreign interest)
  Visits to Contractors - generally not a problem

- LACK OF FOREIGN DISCLOSURE DECISIONS
- NO CONSISTENCY IN PROCEDURES WITHIN OR BETWEEN AGENCIES

Nothing is listed in the table that has not taken place. A horror story! Certainly. But you must remember that the Reciprocal clearance process is new and the regulations for compliance, the interpretation of policy, and the dicta of the politicians or the politics have not reached "the troops" who must carry them out. Also you must remember, that this is a reversal of traditional policy. As of the moment the only countries involved in the reciprocal policy are Canada, the U.K. and the recently added Federal Republic of Germany. The number of countries involved in the industrial security process may be as many as eight. You might remember that I said earlier that a foreign disclosure decision must be made for each country and for each program or project. That indeed is a formidable task, but one that must be done.

However, corrective action is being taken. Companies are being encouraged to challenge any adverse decision involving classification or disclosure, or whether information actually is prohibited from disclosure. This too is different, because companies traditionally do not challenge govern-

ment decisions — they don't want to rock the boat or get procurement activities angry with them. Well, their survival is at stake — if they do not wish to make a fight — so be it. Further, when appropriate, requests are being made that a foreign disclosure decision be reached. Any negative decision made at a command level lower than a Systems Command or a Military Department is challenged. The suggestion is that a negative decision not be made at lower than those levels. To date, there has been considerable success, but much remains to be done.

Acquisitions — The Booby Traps

We are now in a sticky area — one that strikes to the heart of business privacy. However, having been involved in the process, I would like to make some observations which might ease some of the problems.

Traditionally, the possibility of Company A acquiring Company B is information closely held within a small and select circle. Company A does considerable business with the MOD and wants to break into the U.S. defense business. It knows of a good U.S. business which has defense contracts and has a product line compatible with theirs; acquisition would be mutually beneficial.

The Company A people may discuss the acquisition with their opposite numbers in Company B until the major details have been decided on, or, if any others, it is with the lawyers, financial people and the like. Seldom is the subject discussed with the Security Officers of either — frequently, they are the last to know. The arrangements are completed — the acquisition is a fact.

Then the bubble bursts — the U.S. government says NO. Company B may not be acquired by an alien company, or if it is, all defense business will be cancelled, unless positive steps are taken to remove, permanently, all alien influence.

You now might recall earlier remarks on how alien investment is controlled in the U.S. by the industrial security program. While I will not discuss specifics, I do have some suggestions of steps which might be taken to avoid this problem.

Table 9 poses the pertinent questions which might be raised during the decision-making process. The answers might well provide the key to whether an acquisition should or should not proceed. You will note that they are not the usual: cash flow, stock, general business information.

A little background. Under U.S. contracting procedures, R&D can be an allowable contract overhead cost. Although the percentage of defense business to the total company business may be very small, the percentage may represent a major portion of the company's budget for new product development. There are countless examples of this.

TABLE 9

ACQUISITION BOOBY TRAPS AVOIDANCE QUESTIONS

- DOES THE COMPANY DO DEFENSE BUSINESS?
- WHAT IS THE PERCENTAGE OF DEFENSE BUSINESS TO THE TOTAL?
- HOW IMPORTANT IS THAT SHARE? DOES THE SHARE REPRESENT THE COMPANY'S R & D ON NEW PRODUCT DEVELOPMENT?
- WHAT IS THE SENSITIVITY OF THAT PERCENTAGE?
- WHO ARE THE CUSTOMERS?
- WHAT WOULD BE THE EFFECT IF THAT PERCENTAGE WAS LOST TO THE COMPANY OR REDUCED?
- WHAT WOULD BE THE EFFECT ON THE RETENTION OF KEY PERSONNEL?

So the questions should be asked and frequently they are not. Without the questions and the answers, both parties lose, and the situation could have been avoided. Obviously, I am not telling you how to get the answers, but they can be obtained — quietly. The questions have been asked and answered -- a decision is made to proceed with the negotiations. What now?

I am sure that neither you nor your bosses like surprises. Neither do the responsible DoD commands and activities. Therefore, when a decision is made to proceed, I would strongly urge that the top officials of Company A visit the commanders or top people of the DoD, the Military Departments

and the Procurement/Acquisition people of the DoD and inform them of the possible acquisition of Company B by Company A, and seek their opinions.

- Would they approve, disapprove or take no position?
- What would be their position on existing contracts; on future contracts?

Obviously no responsible official could make formal commitments on new contracts, or even give an opinion on the future status of the national disclosure decisions. However, the officials of Company A could get important clues, impressions or whatever on the acquisition.

In sum, the acquisition decision process can be enhanced by prior planning. I will not, of course, give you specific examples; however, having been involved in the process, prior planning can lead to better decisions.

The Future — Prayerfully

This has been a long and complicated discussion. However, all the parts are related and to do one's job, one must know not only the parts, but how they relate. Specifically omitted has been anything about physical security, clearances and the like. Although those subjects are important, we are here talking about information, information which must be identified as requiring protection at what level and for how long. It is information which establishes the need for clearances, locks and keys and the like. Information on how to build a piece of equipment is more important than having the piece.

At the outset NCMS was the subject — what it is, how it fits, its importance and influence in the scheme of things; its membership and where they are in their organizations as well as the breadth of the membership. I am predjudiced, but it is a most useful organization.

Next was the National Disclosure Policy process which is nothing more or less than the definition of the U.S.'s relationship to those countries with which it has Security of Information Agreements and especially those with which there are Industrial Security Annexes to those Agreements. As you all know, foreign affairs are dynamic, fluid, exasperating, and every other adjective which may be appropriate to a given situation. It rarely is static. Whether one agrees or disagrees with a particular policy, one can be equally sure that it will change over time. Yesterday's friends are today's enemies and vice versa. And defense matters follow those policies. Since World War II, for example, each of us has been talking interoperability of equipment. Advances have been tortuous; nonetheless, there have been advances.

Technology transfer is more of an emotional problem than technical. From the earliest days, discoveries were principally of Greco-Roman and European origin, but we tend to forget the contributions of the Arabs in mathematics and the Chinese in computation. In these days of instant communications, the young among us tend to forget (if they ever knew) that there are many examples of similar discoveries made widely by people not necessarily in contact with each other. We also get so upset about "giving away" technology that we tend to forget not only what technology is, but define the term to satisfy a particular purpose. In the final analysis, technology in the U.S. (and I feel in the U.K.) generally is privately owned and developed primarily by private funds. The U.S. government actually owns or controls very little technology.

In the area of Export Controls there are laws and controls such as the International Traffic in Arms Regulation. The principal efforts have been in the control of atomic and atomic related information.

FOCI is controlled by indirection. With the rapid increase in petrodollars and the attractiveness of U.S. business — especially defense — as an investment, there is proper concern about foreign *influence*. Given the temper of the times, I am sure that this concern will continue.

Whether the Voting Trust option, or a Reciprocal clearance is the best road to success is a matter of personal choice. DoD Reciprocal clearances are a problem and now don't really mean much; but conditions are changing for the better.

You know of the efforts made to get the attention of the high levels of the DoD, the NCMS panel at its Florida seminar where the problems were aired publicly. Since then a meeting was held at the British Embassy for U.K. and U.K.-owned companies to hear a DoD presentation on Reciprocal clearances — it resulted from the Florida-seminar Panel. It may be described as a disaster. A result of that meeting was a letter from the Embassy to an Assistant Secretary for Policy, DoD. That letter also stirred the stew and generated more questions. The answers are still being debated.

With all the action being taken, the attention being given by high levels of our governments, I am confident that the situation will improve — given only that we continue to agitate, question, challenge and probe. As an example, I am studying the applicable directives (more than 35) and recommending changes in language to improve relations and make a Reciprocal clearance a viable instrument, keeping in mind that — as in personal matters — there always will be some information which cannot and should not be made available even to the closest of friends. The important point is that the information must be identified *precisely*, the type of protection identified, and the length of time the protection should remain in effect be established.

Finally, and with due apologies to the cognoscent here present, I would quote Claudio in *Much Ado About Nothing*:

> "Friendship is constant in all other things,
> Save in the office and affairs of love;
> Therefore, all hearts in love use their
> own tongues; 'Let every eye negotiate
> for itself and trust no agent'."


DA
FILM